ADMINISTRATION GUIDE

Cisco Small Business

RV 120W Wireless-N VPN Firewall

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

© 2009 Cisco Systems, Inc. All rights reserved.

78-19307-01

Contents

Chapter 1: Introduction 1

Product Overview 1

Getting to Know the Cisco RV 120W 3

Front Panel 3

Back Panel 4

Mounting the Cisco RV 120W 5

Installation Guidelines 5

Wall Mounting 5

Connecting the Equipment 7

Using the Setup Wizard 8

Starting the Wizard 8

Connecting Your Hardware 9

Entering Login and Internet Connection Information 13

Configuring Security 14

Manually Connecting Your System 16

Verifying the Hardware Installation 17

Connecting to Your Wireless Network 17

Getting Started in the Cisco RV 120W Device Manager 18

Logging In 18

Using the Getting Started Page 19

Navigating through the Pages 20

Saving Your Changes 21

Viewing the Help Files 22

Viewing Device Statistics 22

Viewing the System Summary 22

Viewing the Wireless Status 25

Viewing the IPsec Connection Status 26

Viewing the QuickVPN Connection Status 27

Viewing Logs 27

Viewing Available LAN Hosts 28

Viewing the Port Triggering Status 28

Viewing Port Statistics 28

Chapter 2: Configuring Networking 30

Configuring the Wide Area Network (WAN) 30
Configuring the WAN for an IPv4 Network 30
Configuring the Internet Connection Type 30
Configuring Internet Address Information 32
Configuring Domain Name System (DNS) Server Information 33
Configuring Maximum Transmit Unit (MTU) 33
Configuring the Cisco RV 120W Media Access Control (MAC) Address 33
Configuring the WAN for an IPv6 Network 34
Configuring a Static IP Address 34
Configuring DHCPv6 35
Creating PPPoE Profiles 35
Configuring the Local Area Network (LAN) 36
Changing the Default Cisco RV 120W IP Address 37
Configuring DHCP 37
Configuring the LAN DNS Proxy 38
Configuring Virtual LANs (VLANs) 39
Enabling VLANs 39
Creating a VLAN 39
Configuring Port VLANs 40
Associating the Wireless Port to VLANs 41
Configuring Multiple VLAN Subnets 42
Configuring IPv6 LAN Properties 43
Configuring IPv6 Address Pools 44
Configuring LAN Groups 45
Adding a Static IP Address for a Device on the LAN 45
Viewing DHCP Leased Clients 46
Configuring a DMZ Host 46
Configuring Internet Group Management Protocol (IGMP) 47
Configuring Routing 48
Choosing the Routing Mode 48
Viewing Routing Information 48
Configuring Static Routing 49
Configuring Dynamic Routing 50

Configuring Port Management 52
Configuring Dynamic DNS (DDNS) 53
Configuring IPv6 54
Configuring the Routing Mode 54
Configuring IPv6 Static Routing 54
Configuring RIP next generation (RIPng) 55
Configuring IPv6 to IPv4 Tunneling 56
Configuring 6to4 Tunneling 56
Configuring Intra-Site Automatic Tunnel Addressing Protocol Tunnels 56
Viewing IPv6 Tunnel Information 57
Configuring Router Advertisement 57

Chapter 3: Configuring the Wireless Network 60

A Note About Wireless Security 60
Wireless Security Tips 60
General Network Security Guidelines 62
Understanding the Cisco RV 120W's Wireless Networks 63
Configuring Wireless Profiles 63
Configuring the Group Key Refresh Interval 65
Configuring RADIUS Authentication Parameters 66
Configuring Access Points 66
Enabling or Disabling APs 66
Editing an AP's Properties 67
Using MAC Filtering 68
Viewing AP Status 68
Configuring the Wireless Radio Properties 70
Configuring Basic Wireless Radio Settings 70
Configuring Advanced Wireless Radio Settings 71
Configuring Wi-Fi Protected Setup 72
Configuring a Wireless Distribution System (WDS) 73

Chapter 4: Configuring the Firewall 74

Cisco RV 120W Firewall Features 74
Configuring Basic Firewall Settings 76
Protecting from Attacks 76
Configuring Universal Plug and Play (UPnP) 77
Viewing UPnP Information 78
Enabling Session Initiation Protocol Application-Level Gateway (SIP ALG) 78
Configuring the Default Outbound Policy 79
Configuring Firewall Rules 79
Creating a Firewall Rule 80
Managing Firewall Rules 84
Creating Custom Services 84
Creating Firewall Schedules 85
Blocking and Filtering Content and Applications 85
Blocking Web Applications and Components 86
Adding Trusted Domains 87
Adding Blocked Keywords 87
Configuring MAC Address Filtering 88
Configuring IP/MAC Address Binding 89
Firewall Rule Examples 90
Configuring Port Triggering 92
Configuring Port Forwarding 94
Restricting Sessions 97
Configuring Remote Management 98
Configuring One-to-One Network Address Translation (NAT) 99

Chapter 5: Configuring Virtual Private Networks (VPNs) and Security 101

Configuring VPNs 102
Creating Cisco QuickVPN Client Users 102
Using the VPN Wizard 102
Viewing the Default Values 104

Configuring IP Security Policies 105
Configuring IKE Policies 105
Configuring VPN Policies 108
Configuring VPN Clients 113
Monitoring VPN Tunnel Status 113
Configuring IPsec Users 114
Configuring VPN Passthrough 115
Configuring Security 115
Using Certificates for Authentication 115
Uploading CA Certificates 117
Uploading Self Certificates 117
Generating a Self Certificate Request 117
Downloading the Router's Current Certificate 118
Using the Cisco RV 120W With a RADIUS Server 118
Configuring 802.1x Port-Based Authentication 119

Chapter 6: Configuring Quality of Service (QoS) 120

Configuring Bandwidth Profiles 120
Configuring Traffic Flows 121
Configuring Traffic Metering 122
Configuring 802.1p 124
Configuring 802.1p to Queue Mapping 125
Configuring 802.1p CoS to DSCP Remarking 125

Chapter 7: Administering Your Cisco RV 120W 126

Setting Password Complexity 126
Configuring User Accounts 127
Setting the Timeout Value 128
Configuring Simple Network Management (SNMP) 128
Editing SNMPv3 Users 128
Adding SNMP Traps 129
Configuring Access Control Rules 129
Configuring Additional SNMP Information 130

Using Diagnostic Tools 130
Using PING 131
Using Trace Route 131
Performing a DNS Lookup 131
Capturing and Tracing Packets 131
Configuring Logging 131
Configuring Local Logging 132
Configuring Remote Logging 133
Configuring the Logging Type and Notification 134
Configuring E-Mailing of Log Events 135
Configuring Discovery (Bonjour) 135
Configuring VLAN Associations 136
Configuring Date and Time Settings 136
Backing Up and Restoring the System 137
Upgrading Firmware 138
Rebooting the Cisco RV 120W 138
Restoring the Factory Defaults 138

Appendix A: Using Cisco QuickVPN for Windows 2000, XP, or Vista 139

Overview 139
Before You Begin 139
Installing the Cisco QuickVPN Software 140
Installing from the CD-ROM 140
Downloading and Installing from the Internet 142
Using the Cisco QuickVPN Software 142

Appendix B: Where to Go From Here 146

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 1**
- **Getting to Know the Cisco RV 120W, page 3**
- **Mounting the Cisco RV 120W, page 5**
- **Connecting the Equipment, page 7**
- **Verifying the Hardware Installation, page 17**
- **Getting Started in the Cisco RV 120W Device Manager, page 18**

Product Overview

Thank you for choosing the Cisco Small Business RV 120W Wireless-N VPN Firewall. The Cisco RV 120W 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 Cisco RV 120W provides a Wireless-N access point, combined with support for Virtual Private Networks (VPNs) to make your network more secure. Its 10/100 Ethernet WAN interface connects directly to your broadband DSL or Cable modem. There are four full-duplex 10/100 Ethernet LAN interfaces that can connect up to four devices. The wireless access point supports the 802.11n standard with MIMO technology, which multiplies the effective data rate. This technology results in better throughput and coverage than provided by 802.11g networks.

The Cisco RV 120W incorporates a Stateful Packet Inspection (SPI)-based firewall with Denial of Service (DoS) prevention and a Virtual Private Network (VPN) engine for secure communication between mobile or remote workers and branch offices. The Cisco RV 120W supports up to ten gateway-to-gateway IP Security (IPsec) tunnels to facilitate branch office connectivity through encrypted virtual links. Users connecting through a VPN tunnel are attached to your company's network with secure access to files, e-mail, and your intranet as if they were in the building. You can also use the VPN capability to allow users on your small office network to securely connect out to a corporate network

The Cisco RV 120W's wireless access point supports Wireless Distribution System (WDS), which allows the wireless coverage to be expanded without wires. It also supports multiple SSIDs for the use of virtual networks (up to 4 separate virtual networks), with 802.1Q-based VLAN support for traffic separation. The Cisco RV 120W implements WPA2-PSK, WPA2-ENT, and WEP encryption, along with other security features including the disabling of SSID broadcasts, MAC-based filtering, and allowing or denying "time of day" access per SSID. The Cisco RV 120W supports Wi-Fi Multimedia (WMM) and Wi-Fi Multimedia Power Save (WMM-PS) for wireless Quality of Service (QoS). It supports 802.1p, Differentiated Services Code Point (DSCP), and Type of Service (ToS) for wired QoS, which can improve the quality of your network when using delay-sensitive Voice over IP (VoIP) applications and bandwidth-intensive video streaming applications.

With the Cisco RV 120W's embedded web server, its settings can be configured using the browser-based Device Manager. The Cisco RV 120W supports Internet Explorer, Firefox, and Safari web browsers. The Cisco RV 120W also provides a setup wizard and VPN wizard. The setup wizard allows you to easily configure the Cisco RV 120W's basic settings. You can use the VPN wizard to easily configure VPN tunnels.

Getting to Know the Cisco RV 120W

Front Panel

POWER—The Power LED lights up green to indicate the device is powered on. Flashes green when the power is coming on or software is being upgraded.

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

WIRELESS—The Wireless LED lights up green when the wireless module is enabled. The LED is off when the wireless module is disabled. The LED flashes green when the device is transmitting or receiving data on the wireless module.

LAN—These four LEDs correspond to the four LAN (Ethernet) ports of the Cisco RV 120W. If the LED is continuously lit green, the Cisco RV 120W is connected to a device through the corresponding port (1, 2, 3, or 4). The LED for a port flashes green when the Cisco RV 120W is actively sending or receiving data over that port.

Back Panel

RESET Button—The Reset button has two functions:

- If the Cisco RV 120W is having problems connecting to the Internet, press the **RESET** button for less than five 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 are experiencing extreme problems with the Cisco RV 120W and have tried all other troubleshooting measures, press and hold in the **RESET** button for 10 seconds. This will restore the factory defaults and clear all of the Cisco RV 120W settings.

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

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

ON/OFF Power Switch—Press this button to turn the Cisco RV 120W on and off. When the button is pushed in, power is on.

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

Mounting the Cisco RV 120W

You can place your Cisco RV 120W on a desktop or mount it on a wall.

Installation Guidelines

- **Ambient Temperature**—To prevent the device 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 device.
- **Mechanical Loading**—Be sure that the device is level and stable to avoid any hazardous conditions.

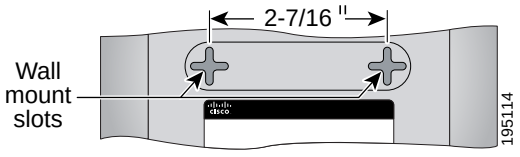
For desktop placement, place the Cisco RV 120W device horizontally on a flat surface so that it sits on its four rubber feet.

Wall Mounting

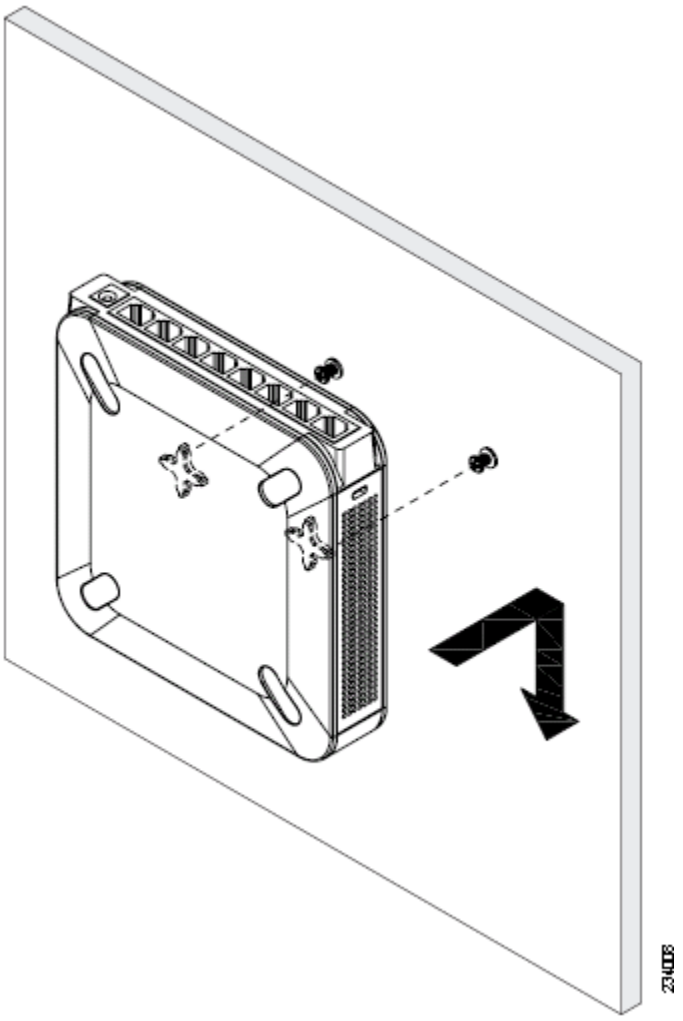
STEP 1 Determine where you want to mount the device and install two screws (not supplied) that are 2-7/16 in. apart (approximately 61 mm). Mounting screws should have a head that is approximately 5.5 mm in diameter and 2 mm deep, with a shaft that is at least15.5 mm long and approximately 3.5 mm wide. (Your wall may require shorter or longer screws, or drywall anchors.)

Do not mount the screw heads flush with the wall; the screw heads must fit inside the back of the device.

STEP 2 With the back panel pointing up (if installing vertically), line up the device so that the wall-mount slots on the bottom of the device line up with the two screws.



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



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 Setup Wizard or the Device Manager. The Setup Wizard is supported on Microsoft Windows 2000, Windows XP, Windows Vista, and Windows 7. You must have Microsoft Core XML Services (MSXML) software installed on the PC to run the Setup Wizard. MSXML is available from the following location:

  http://www.microsoft.com/windows/downloads/

  The Device Manager is supported on the following web browsers:

  - Microsoft Internet Explorer 6.0 and later
  - Mozilla Firefox 3.0 and later
  - Apple Safari 3.0 or later.
- Ethernet cable (provided) to connect the PC to the router for configuration.
- Software CD containing Setup Wizard (provided).

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.

Cisco recommends that you use the Setup Wizard to connect and configure your Cisco RV 120W. If you do not want to use the setup wizard, skip to the **"Manually Connecting Your System" section on page 16**.

Using the Setup Wizard

Follow these steps to use the Cisco RV 120W Setup Wizard. The Setup Wizard displays on-screen instructions that guide you through the installation, but you may find it useful to refer to this document during installation.

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

Starting the Wizard

STEP 1 Make sure that all of the network hardware is powered off, including the Cisco RV 120W and cable or DSL modem.

STEP 2 Insert the CD that shipped with the Cisco RV 120W into the PC you are using to configure the Cisco RV 120W. The Setup Wizard automatically begins.

STEP 3 Click **Start** to begin the installation.

STEP 4 Click the check box to accept the software license agreement and click **Next**.

STEP 5 The Setup Wizard verifies the network adapter on your PC is functional. If you receive an error, view your PC's network connections to make sure the network adapter is working and click **Back** to test the connection again.

Next:

- If your network adapter is functional and you have not yet connected your hardware, the **Install Router** window appears. (See **Connecting Your Hardware, page 9**.)
- If your network adapter is functional, you have already connected your hardware, and your Internet connection has been detected, the **Secure Your Router Settings** window appears. (See **Configuring Security, page 14**.)

Connecting Your Hardware

STEP 1 You should have an Ethernet cable connecting your PC to the cable or DSL modem. Unplug one end of the cable from your PC and plug it into the port marked "WAN" on the device. Click **Next**.

STEP 2 Connect one end of a different Ethernet cable to one of the LAN (Ethernet) ports on the back of the device. (In this example, the LAN 2 port is used.) Connect the other end to an Ethernet port on the PC that is running the Setup Wizard. Click **Next**.

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

STEP 4 Connect the power adapter to the Cisco RV 120W power port. Click **Next**.

CAUTION Use only the power adapter that is supplied with the device. Using a different power adapter could damage the device.

STEP 5 Plug the other end of the adapter into an electrical outlet.

STEP 6 On the Cisco RV 120W, push in the ON/OFF POWER SWITCH button. The Setup Wizard searches for the Cisco RV 120W.

The POWER LED on the front panel lights up green when the power adapter is connected properly and the device is turned on.

Next:

- If your hardware connection is successful, but the Setup Wizard needs more information about your Internet connection, the **Enter Username and Password** window appears. (See **Entering Login and Internet Connection Information, page 13**.)
- If your hardware connection is successful and the Setup Wizard successfully detects your Internet connection, the **Configure Router** window displays. (See **Configuring Security, page 14**.)

Entering Login and Internet Connection Information

STEP 1 Enter the username and password for your Cisco RV 120W. The default username and password are both **admin**. Click **Next**.

STEP 2 Choose your Internet connection type:

- Telephone (DSL)
- Cable broadband
- I don't know

Click **Next**.

STEP 3 The Setup Wizard confirms your Internet connection settings. If it cannot detect or confirm your settings, you might need to provide information about your Internet connection type. You can get this information from your ISP.

The types of Internet connections are:

- **Dynamic (DHCP)**—Your PC receives its IP address from your cable or DSL modem. This address can change.
- **Static IP Connection**—Your Internet Service Provider (ISP) has assigned you an IP address that does not change. You will need this address and some additional information (see Step 4) to proceed with installation.
- **PPPoE**—You have a point-to-point connection to the Internet (used mainly with asymmetric DSL).
- **PPTP**—Your provider uses point-to-point tunneling protocol (used in Europe).
- **LT2P**—Your provider uses layer 2 tunneling protocol (used in Europe).

After selecting your connection type, click **Next**.

STEP 4 If you chose:

- **Dynamic (DHCP)**—Proceed to Step 5.
- **Static IP Connection**—Provide your Static IP Address, Subnet Mask, Gateway IP, DNS, and secondary DNS (optional). This information comes from your ISP. Click **Next** after entering the information.
- **PPPoE**—Provide your account name (for example, *john@ISPname.net*), and password. Click **Next** after entering the information.

- **PPTP (Europe)**—Provide your account name (for example, *john@ISPname.net*), password, and server IP address. Click **Next** after entering the information.
- **L2TP (Europe)**—Provide your account name (for example, john@ISPname.net), password, and server IP address. Click **Next** after entering the information.

STEP 5 The Setup Wizard configures your connection, verifies the router settings, and checks the network connection. Click **Next**.

STEP 6 To configure your home network, click **Next**.

Configuring Security

STEP 1 Enter a new Cisco RV 120W administration password and click **Next**. For security reasons, you should not use the default password. Follow these password guidelines:

- Passwords should not contain dictionary words from any language or the default password.
- Passwords should contain a mix of letters (both upper- and lowercase), numbers, and symbols.
- Passwords must be at least 8 but no more than 30 characters.
- Password security ratings are shown to the right of the password you enter, and are rated from weak to secure. Cisco recommends using a password rated as secure.

STEP 2 Enter a name (SSID) for your wireless network and click **Next**. You should change the default SSID to a unique name. The SSID is case-sensitive.

NOTE For added security, disable broadcasting of the SSID. You can disable SSID broadcast using the Device Manager; see **Editing an AP's Properties, page 67**.

STEP 3 Select the type of security to use:

Best Security (WPA2)

Strong wireless security that uses a password (security key) to protect your network. Recommended for most networks. The devices you connect to your wireless network must support WPA2; see the support information for your device if you have questions.

a. Enter a security key (must be at least 8 and no more than 63 characters) or use the randomly-generated one provided by the Cisco RV 120W. Keys should contain a mix of letters (both upper- and lowercase), numbers, and symbols. Security key ratings are shown to the right of the password you enter, and are rated from weak to secure. Cisco recommends using a password rated as secure.

b. Click **Next**.

Better Security (WPA)

Wireless security that uses a password (security key) to protect your network. It is less secure than WPA2, but it is supported by older devices. If the devices you are connecting to your wireless network do not support WPA2, choose this option.

a. Enter a security key (must be at least 8 and no more than 63 characters) or use the randomly-generated one provided by the Cisco RV 120W. Keys should contain a mix of letters (both upper- and lowercase), numbers, and symbols. Security key ratings are shown to the right of the password you enter, and are rated from weak to secure. Cisco recommends using a password rated as secure.

b. Click **Next**.

No Security

This option is not recommended; it allows devices to connect to your wireless network if the network name is known.

a. Click **Next**.

b. Click **Yes** when the warning message is displayed.

STEP 4 The security settings for your network are shown. To save these settings in a text file on your PC, check the box provided. To print, click **Print these settings**. Click **Next** to confirm these settings. (If you chose to save these settings to your desktop, then click **OK**.)

NOTE You must enter this security information on each device that connects to your network. Save this information!

STEP 5 The Cisco RV 120W configures your connection and displays a status message if the configuration is successful. Click **Next**.

STEP 6 The Cisco RV 120W displays a message if it has been configured and is successfully connected to the Internet. Click **Finish**.

Manually Connecting Your System

Use these procedures if you do not want to use the Setup Wizard.

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

STEP 1 Connect your equipment as described in **"Connecting Your Hardware" section on page 9**.

STEP 2 Connect to the Device Manager to view and configure your Cisco RV 120W settings. When you connect to the Device Manager, the Getting Started page shows links that you can click to perform basic tasks. At a minimum, we recommend that you:

- Change the Cisco RV 120W password (see **Configuring User Accounts, page 127**.)
- Review wireless profile and set security settings (see **Configuring the Wireless Radio Properties, page 70**.)

See the "Getting Started in the Cisco RV 120W Device Manager" section on page 18 for more information.

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 RV 120W, page 3.
- 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 17.

Connecting to Your Wireless Network

To connect a device (such as a PC) to your wireless network, you must configure the wireless connection with the security information you entered when you used the Setup Wizard or that 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) you chose for your network when you configured the Cisco RV 120W.

STEP 3 Choose the type of encryption and enter the security key that you chose when setting up the Cisco RV 120W. If you did not enable security (not recommended), leave these fields blank.

STEP 4 Verify your wireless connection and save your settings.

Getting Started in the Cisco RV 120W Device Manager

The Device Manager allows you to configure and manage your Cisco RV 120W, including the following tasks:

- View system status information
- Configure local and wide-area network settings
- Configure wireless security, firewall, and VPN settings
- Configure quality of service
- Perform software upgrades

Logging In

To use the Device Manager:

STEP 1 On a PC connected to a LAN port on the back panel of the Cisco RV 120W, start your web browser. (If you have performed the initial configuration using the Setup Wizard, you can connect using the Cisco RV 120W's wireless connection.)

STEP 2 To connect to the Device Manager, enter **http://192.168.1.1** in your browser's address field, and press **Enter**. A password request page appears.

NOTE The default IP address is 192.168.1.1. If there is another device connected to the network that is acting as a DHCP server, that device may assign a different address to the Cisco RV 120W. You must use the assigned IP address to connect to the Cisco RV 120W.

STEP 3 In the Username and Password fields, enter the default user name (which is **admin**) and password (which is also **admin**), in lowercase letters. Then 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

- Change Default Administrator Password—See **Configuring User Accounts, page 127**.
- Configure WAN Settings—See **Configuring the WAN for an IPv4 Network, page 30**.
- Configure LAN Settings—See **Configuring the Local Area Network (LAN), page 36**.
- Review Wireless Profile and Set Security Settings—See **Configuring Access Points, page 66**.
- Add VPN Clients—See **Configuring IPsec Users, page 114**.

Quick Access

- Upgrade Device Software—See **Upgrading Firmware, page 138**.
- Configure Site to Site VPN—See **Using the VPN Wizard, page 102**.
- Configure Remote Management Access—See **Configuring Remote Management, page 98**.

Device Status

- System Summary—See **Viewing Device Statistics, page 22**.
- Wireless Status—See **Viewing the Wireless Status, page 25**.
- VPN Status—See **Viewing the IPsec Connection Status, page 26**.

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

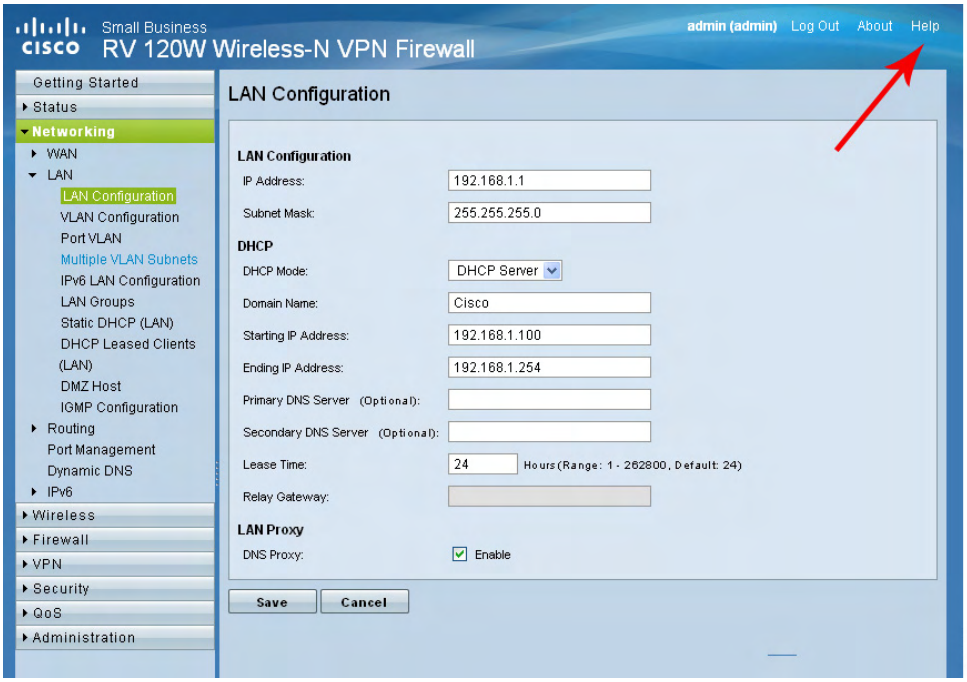
Use the navigation tree in the left pane to open the configuration pages. Click a menu item on the left panel to expand it. Click the menu names displayed underneath to perform an action or view a sub-menu.

Saving Your Changes

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

Viewing the Help Files

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



Viewing Device Statistics

The Cisco RV 120W provides real-time statistics for the device. To access statistics, in the Device Manager, choose **Status**.

Viewing the System Summary

To view the system summary, choose **Status** > **System Summary**. Click **Refresh** to refresh the information and obtain the latest information.

The system summary page 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.
- **CPU Usage**—Percentage of CPU currently used.
- **Memory Usage**—Percentage of memory currently used.

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 if 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 if the device is acting as a DHCP relay (DHCP relay must be enabled).
- **DHCPv6 Server**: Indicates if 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 if 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

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.

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.

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 Status

This page 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 transmitted/received (tx/rx) bytes of information reported to the radio, over all configured APs.
- **Errors**—The number of transmitted/received (tx/rx) packet errors reported to the radio, over all configured APs.
- **Dropped**—The number of transmitted/received (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 transmitted/received (tx/rx) wireless packets on the AP.
- **Bytes**—The number of transmitted/received (tx/rx) bytes of information on the AP.
- **Errors**—The number of transmitted/received (tx/rx) packet errors reported to the AP.
- **Dropped**—The number of transmitted/received (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

This page 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

This page 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

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

This page shows available LAN hosts.

Viewing the Port Triggering Status

The Port Triggering Status page 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 Port Statistics

This table 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 router and refresh the page automatically. To modify the poll interval, click the **Stop** button and then **Start** to restart automatic refresh.

2

Configuring Networking

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

- Configuring the Wide Area Network (WAN), page 30
- Configuring the Local Area Network (LAN), page 36
- Configuring Routing, page 48
- Configuring Routing, page 48
- Configuring Dynamic DNS (DDNS), page 53
- Configuring IPv6, page 54

Configuring the Wide Area Network (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

Configuring WAN properties for an IPv4 network differs depending on which type of Internet connection you have. See the sections below for detailed instructions.

Configuring the Internet Connection Type

NOTE If your Internet connection does not require a login, you do not need to configure the ISP Connection Type fields.

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

STEP 2 If you connect to the Internet using one of the following connection types, check the **Internet Connection Requires a Login** box:

- Point-to-Point Protocol over Ethernet (PPPoE)—used mainly with asymmetric DSL.
- Point-to-Point Tunneling Protocol (used in Europe).
- Layer 2 Tunneling Protocol (used in Europe).

STEP 3 Choose your ISP Connection Type:

PPPoE

a. First, create a PPPoE Profile. See **"Creating PPPoE Profiles" on page 35**.

b. Under PPPoE Profile Name, select the profile you created on the **WAN** > **PPPoE Profiles** page. The username, password, and other fields are entered automatically.

c. Go to **"Configuring Maximum Transmit Unit (MTU)" on page 33**.

PPTP

a. Provide your username and password. These are assigned to you by the ISP to access your account.

b. If your ISP supports Microsoft Point-to-Point encryption, check the **MPPE Encryption** box.

c. Choose the connectivity type:

- **Keep connected**—The Internet connection is always on.
- **Connect on demand**—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.

d. Enter the IP address assigned to you by your ISP in the **My IP Address** field.

e. Enter the IP address of your ISP's server in the **Server IP Address** field.

f. Go to **"Configuring Maximum Transmit Unit (MTU)" on page 33**.

L2TP

a. Provide your username and password. These are assigned to you by the ISP to access your account.

b. Enter your secret phrase. This phrase is known to you and your ISP for use in authenticating your logon.

c. Choose the connectivity type:

- **Keep connected**—The Internet connection is always on.
- **Connect on demand**—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.

d. Enter the IP address assigned to you by your ISP in the **My IP Address** field.

e. Enter the IP address of your ISP's server in the **Server IP Address** field.

f. Click **Save**. If applicable, go to **"Configuring Maximum Transmit Unit (MTU)" on page 33**.

Configuring Internet Address Information

STEP 1 If your ISP uses Dynamic Host Control Protocol (DHCP) to assign you an IP address, you receive a dynamic IP address that is newly generated each time you log in. In the IP Address Source field, choose **Get Dynamically From ISP**.

If your ISP has assigned you a static (non-changing) IP address, in the IP Address Source Field, choose **Use Static IP Address** and enter the following:

- IP address assigned to you by your ISP.
- IPv4 subnet mask assigned to you by your ISP.
- ISP gateway's IP address.

STEP 2 Click **Save**.

Configuring Domain Name System (DNS) Server Information

DNS servers map Internet domain names (for example, www.cisco.com) to IP addresses. Under DNS Server Source, you can choose whether to get DNS server addresses automatically from your ISP or to use ISP-specified DNS server addresses.

STEP 1 If your ISP provides DNS servers, under DNS Server Source, choose **Get Dynamically from ISP**.

If your ISP instructs you to use specific DNS server addresses, under DNS Server Source, choose **Use These DNS Servers**. Enter the IP address of the primary and secondary DNS servers.

STEP 2 Click **Save**.

Configuring Maximum Transmit Unit (MTU)

The MTU (Maximum Transmit Unit) 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 RV 120W Media Access Control (MAC) Address

The router has a unique 48-bit local Ethernet hardware address. In most cases, the default MAC address is used to identify your Cisco RV 120W 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 router.

- **Use This MAC Address**—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

Configuring WAN properties for an IPv6 network differs depending on which type of Internet connection you have. See the sections below for detailed instructions.

NOTE Before configuring any WAN properties for an IPv6 network, you must configure the routing mode. Choose **Networking** > **IPv6** > **Routing Mode** and select IPv4 / IPv6 mode. Click **Save**.

The Cisco RV 120W can be configured to be a DHCPv6 client of the ISP for this WAN or a static IPv6 address provided by the ISP can be assigned.

Configuring a Static IP Address

If your ISP assigns you a fixed address to access the Internet, choose this option. The information needed for configuring a static IP address can be obtained from your ISP.

STEP 1 In the **Internet Address** field, choose **Static IPv6**.

STEP 2 Enter the IPv6 IP address assigned to your router.

STEP 3 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 4 Enter the default IPv6 gateway address, or the IP address of the server at the ISP that this router will connect to for accessing the internet.

STEP 5 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 6 Choose the method by which the router obtains an IP address:

STEP 7 Click **Save**.

Configuring DHCPv6

When the ISP allows you to obtain the WAN IP settings via DHCP, you need to provide details for the DHCPv6 client configuration.

STEP 1 In the Internet Address field, choose **DHCPv6**.

STEP 2 Choose if the DHCPv6 client on the gateway is stateless or stateful. If a stateful client is selected, the gateway connects to the ISP's DHCPv6 server for a leased address. For stateless DHCP, it is not necessary to have a DHCPv6 server available at the ISP. Instead, a ICMPv6 discover messages will originate from the Cisco RV 120W and is used for auto-configuration.

STEP 3 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 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 router then sends back authentication credentials with the security type sent earlier by the server.

- **PAP**—The Cisco RV 120W uses Password Authentication Protocol when connecting with the ISP.
- **CHAP**—The Cisco RV 120W uses Challenge Handshake Authentication Protocol when connecting with the ISP.
- **MS-CHAP** or **MS-CHAPv2**—The Cisco RV 120W 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 Local Area Network (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 router 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 router 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 firewall to act as a gateway to additional logical subnets on your LAN. You can assign the firewall an IP address on each additional logical subnet.

NOTE If you have IPv6 configured, see **"Configuring IPv6 LAN Properties" on page 43**.

Changing the Default Cisco RV 120W IP Address

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

STEP 2 In the IP address field, enter the new IP address for your Cisco RV 120W. 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 RV 120W. You must do one of the following:

- Release and renew the IP address on the PC that you are using to access the Cisco RV 120W (if DHCP is configured on the router).
- Manually assign an IP address to your PC that is in the same subnet as the Cisco RV 120W. For example, if you change the Cisco RV 120W 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 RV 120W to re-connect.

Configuring DHCP

By default, the Cisco RV 120W 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 router'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 RV 120W 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 router'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 RV 120W. 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 In the LAN Proxy section, to enable the Cisco RV 120W to act as a proxy for all DNS requests and communicate with the ISP's DNS servers, check **Enable DNS Proxy**. When this feature is enabled, the router acts as a proxy for all DNS requests and communicates with the ISP's DNS servers (as configured in the WAN settings page). All DHCP clients receive the Primary/Secondary DNS IP and the IP of the router where DHCP is running. All DHCP clients receive the DNS IP addresses of

the ISP, excluding the DNS Proxy IP address when it is disabled. The feature is useful for an "auto rollover" configuration. For example, if the DNS servers for each connection are different, then a link failure can render the DNS servers inaccessible. However, when the DNS proxy is enabled, then clients can make requests to the router and the router, in turn, sends those requests to the DNS servers of the active connection.

STEP 3 Click **Save**.

Configuring Virtual LANs (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 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 routing between this and other VLANS, check the **Inter VLAN Routing Enable** box.

STEP 6 Click **Save**.

Configuring Port VLANs

You can associate VLANS on the Cisco RV 120W 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:

- **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 RV 120W is tagged. Data passing through the phone from a connected device is untagged.

- **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.

- **Trunk mode**—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 **General** or **Access** mode, enter the default Port VLAN ID (PVID). This ID is used to tag untagged packets that come into the port.

STEP 5 Click **Save**.

NOTE If you have changed the port mode, you must save the change and return to the Port VLAN list before configuring the VLAN membership. Check the box next to the port and click **Edit**.

STEP 6 If you selected **General** or **Trunk** mode, you can assign the LAN port to one or more VLANs by checking the box next to the VLAN.

STEP 7 Click **Save**.

Associating the Wireless Port to VLANs

You can associate wireless VLANS on the Cisco RV 120W 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:

- **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 RV 120W is tagged. Data passing through the phone from a connected device is untagged.

- **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.

- **Trunk mode**—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 **General** or **Access** mode, enter the default Port VLAN ID (PVID). This ID is used to tag untagged packets that come into the port.

STEP 5 Click **Save**.

NOTE If you have changed the port mode, you must save the change and return to the Port VLAN list before configuring the VLAN membership. Check the box next to the port and click **Edit**.

STEP 6 If you selected **General** or **Trunk** mode, you can assign the LAN port to one or more VLANs by checking the box next to the VLAN.

STEP 7 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 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 RV 120W by the LAN port that is a member of this VLAN, you might have to release and renew the IP address on the PC connected to the LAN port, or manually assign an IP address to your PC that is in the same subnet as the VLAN. Open a new browser window and re-connect to the Cisco RV 120W.

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 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 VLAN's 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**—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 (similar to IPv4 mode). 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 RV 120W. 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 enabled, the Cisco RV 120W assigns an IP address within the specified range plus additional specified information to any LAN endpoint that requests DHCP-served addresses.

STEP 5 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 RV 120W. In this case, the router advertisement daemon (RADVD) must be configured on this device and ICMPv6 router 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.

STEP 6 (Optional) Enter the domain name of the DHCPv6 server.

STEP 7 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.

STEP 8 Choose the DNS proxy behavior:

- **Use DNS Proxy**—Check this box to enable DNS proxy on this LAN, or uncheck this box to disable this proxy. When this feature is enabled, the router 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.

STEP 9 Enter the lease/rebind time. Enter the duration (in seconds) for which IP addresses will be leased to endpoints on the LAN.

STEP 10 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 RV 120W'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 List of Address Pools field, 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**.

Configuring LAN Groups

You can create LAN groups, which are groups of endpoints that are identified by their IP address. After creating a group, you can then configure actions, such as blocked keywords in a firewall rule, that apply to the group. (See **Adding Blocked Keywords, page 87**.)

To create a LAN Group:

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

STEP 2 Click **Add**.

STEP 3 Enter the group name; spaces and quotes are not supported. Click **Save**.

STEP 4 In the LAN Groups page, click the box next to the group you just created and click **Host List**.

STEP 5 To add endpoints to the group, click **Add**.

STEP 6 Enter the IP address of the endpoint and click **Save**. Repeat steps 4 through 6 for each endpoint you want to add to the group.

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.

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 RV 120W supports DMZ options. A DMZ is a sub-network that is open to the public but behind the firewall. 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. Firewall 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 router'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 firewall rules for the zone. See **Configuring Firewall Rules, page 79**.

Configuring Internet Group Management Protocol (IGMP)

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 router and other nodes in the network.

STEP 3 Click **Save**.

Configuring Routing

Choosing the Routing Mode

The Cisco RV 120W 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 router is configured with a single “public” IP address. The Cisco RV 120W 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 RV 120W 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 49**, or **Configuring Dynamic Routing, page 50**.

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 firewall settings on your router in NAT mode, selecting “router” changes those settings back to the default.

Viewing Routing Information

To view routing information your network, choose **Networking** > **Routing** > **Routing Table**. Information about your network routing is displayed, including the following:

- 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.

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

STEP 3 Enter the route name.

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

STEP 5 Check the **Private** 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** or **LAN**).

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

RIP (Routing Information Protocol, RFC 2453) is an Interior Gateway Protocol (IGP) that is commonly used in internal networks. It allows the router 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 RV 120W.

To configure dynamic routing:

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

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

- **Both**—The router both broadcasts its routing table and also processes RIP information received from other routers.
- **Out Only**—The router broadcasts its routing table periodically but does not accept RIP information from other routers.
- **In Only**—The router accepts RIP information from other router, but does not broadcast its routing table.
- **None**—The router neither broadcasts its route table nor does it accept any RIP packets from other routers. 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. It acts as a security feature because routes are exchanged only with trusted routers in the network. RIP authentication is disabled by default. You can enter two key parameters so that routes can be exchanged with multiple routers 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 Auth Key**—Input the auth key for this MD5 key, the auth key that is encrypted and sent along with the RIP-V2 message.
- **Not Valid Before**—Enter the start date when the auth key is valid for authentication.
- **Not Valid After**—Enter the end date when the auth key is valid for authentication.

STEP 5 Click **Save**.

Configuring Port Management

The Cisco RV 120W has four LAN ports. 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 router 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** or **100 Mbps**. The default setting is 100 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. In this case, the endpoint also uses 10 Mbps mode either by auto-negotiation or manual setting.

STEP 6 Click **Save**.

Configuring Dynamic DNS (DDNS)

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

The router will notify dynamic DNS 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. This option can be enabled here if not done on the DynDNS Web site.

e. Check the **Update Every 30 Days** box to configure the router 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 router 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 router is performed in several sections on your Cisco RV 120W. Make sure you do the following:

- Configure IPv6 WAN properties—See **Configuring the WAN for an IPv6 Network, page 34**.
- Set the Routing Mode to IPv4/IPv6 mode. See **Configuring the Routing Mode, page 54**.

Configuring the Routing Mode

To configure IPv6 properties on the Cisco RV 120W, set the routing mode to IPv6:

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

STEP 2 Select **IPv4/IPv6** and click **Save**.

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

STEP 3 Enter the route name.

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

RIPng (RFC 2080) is a routing protocol based on the distance vector (D-V) algorithm. RIPng uses UDP packets to exchange routing information through port 521. RIPng uses a hop count to measure the distance to a destination. The hop count is referred to as metric, or cost. The hop count from a router to a directly-connected network is 0. The hop count between two directly-connected routers is 1. When the hop count is greater than or equal to 16, the destination network or

host is unreachable. By default, the routing update is sent every 30 seconds. If the router receives no routing updates from a neighbor after 180 seconds, the routes learned from the neighbor are considered as unreachable. After another 240 seconds, if no routing update is received, the router will remove these routes from the routing table.

On the Cisco RV 120W, RIPng is disabled by default.

To configure RIPng:

STEP 1 Select **Networking** > **IPv6** > **Routing (RIPng)**.

STEP 2 Check the **Enable RIPng** box.

STEP 3 Click **Save**.

Configuring IPv6 to IPv4 Tunneling

The Cisco RV 120W provides several IPv6 tunneling methods.

Configuring 6to4 Tunneling

6to4 tunneling allows IPv6 packets to be transmitted over an IPv4 network. 6to4 tunneling is typically used when a site or end user wants to connect to the IPv6 Internet using the existing IPv4 network.

To configure 6to4 Tunneling:

STEP 1 Select **Networking** > **IPv6** > **6to4 Tunneling**.

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

STEP 3 Click **Save**.

Configuring Intra-Site Automatic Tunnel Addressing Protocol Tunnels

Intra-site automatic tunnel addressing protocol is a method to transmit IPv6 packets between dual-stack nodes over an IPv4 network. The Cisco RV 120W 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 RV 120W. The endpoint can be the LAN interface (if the LAN is configured as an IPv4 network), or a specific 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**.

Viewing IPv6 Tunnel Information

To view IPv6 tunnel information, choose **Networking** > **IPv6** > **IPv6 Tunnels Status**.

The page displays information about the automatic tunnel set up through the dedicated WAN interface. The table shows the name of tunnel and the IPv6 address that is created on the device.

Configuring Router Advertisement

The Router Advertisement Daemon (RADVD) on the Cisco RV 120W listens for router solicitations in the IPv6 LAN and responds with router advertisements as required. This is stateless IPv6 auto configuration, and the Cisco RV 120W 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 (router advertisements [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 lifetime 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:

- A Note About Wireless Security, page 60
- Understanding the Cisco RV 120W's Wireless Networks, page 63
- Configuring Access Points, page 66
- Configuring the Wireless Radio Properties, page 70
- Configuring the Wireless Radio Properties, page 70
- Configuring Wi-Fi Protected Setup, page 72
- Configuring a Wireless Distribution System (WDS), page 73

A Note About Wireless Security

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

- Wireless Security Tips, page 60
- General Network Security Guidelines, page 62

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.

- Change the default password

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

- Enable MAC address filtering

  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.

- Enable encryption

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

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

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

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

General Network Security Guidelines

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

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

Understanding the Cisco RV 120W's Wireless Networks

The Cisco Small Business RV 120W Wireless-N VPN Firewall provides four Wireless Access Points (APs), or virtual wireless networks. 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 RV 120W, but only one profile is assigned to each AP at a time.

The Cisco RV 120W 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 **A Note About Wireless Security, page 60**.

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 preshared key (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/WPA2

a. Select the encryption method to be used: **TKIP**, **AES**, or **TKIP+AES**.

b. Select the authentication method to be used: **RADIUS**, **PSK**, or **PSK + RADIUS**.

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

d. (Optional) Check the **Enable Pre-Authentication** box to enable pre-authentication for this profile. Pre-authentication allows wireless clients to quickly switch between connected Access Points sharing the same security configuration. This is mainly used when APs are configured with WPA/WPA2 security. In event of wireless client disconnecting from an AP, a notification is sent to the AP, which then sends the pre-authentication info to other APs in the network.

WEP

In the WEP Index and Keys section:

a. In the Authentication field, choose **Open System** or **Shared Key**. If you choose open system, a wireless client doesn't need to provide a shared key in order to access the wireless network. Any client can associate to the router. If you choose shared key, a 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 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 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, click the check 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 RV 120W.

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 70**.

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 8. 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** box to separate this AP into its own network. When this feature is enabled, the AP can communicate with the Cisco RV 120W, but not with any other AP on the network.

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 AP Policy Status field, choose the type of access to the AP:

- **Open**—Access to the network is open to all endpoints and is not allowed or denied based on the endpoint's MAC address. This is the default setting.
- **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 endpoint to allow or deny and click **Save**. The address is added to the table. Repeat this step for all the endpoints 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 **List of Available Access Points**, 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 RV 120W.

Configuring Basic Wireless Radio Settings

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

STEP 2 Select the **Wireless Network Mode**:

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

STEP 3 Select the channel bandwidth. Available choices depend on the wireless network mode chosen in Step 2.

STEP 4 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**. This field is only available when channel spacing is set to **auto**. The signal components above the carrier frequency constitute the upper sideband (USB) and those below the carrier frequency constitute the lower sideband (LSB).

STEP 5 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 RV 120W determine the best channel to use based on the environment noise levels for the available channels.

STEP 6 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 RV 120W 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 RV 120W’s ability to catch all wireless transmissions but severely decreases performance.

STEP 8 (Optional) Check the **U-APSD** 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 Wi-Fi Protected Setup

You can configure Wi-Fi Protected Setup (WPS) on the Cisco RV 120W to allow WPS-enabled devices to more easily connect to the wireless network.

STEP 1 Choose **Wireless** > **WPS**.

STEP 2 Select the AP on which you want to enable WPS. The AP must use WPA, WPA2, or WPA+WPA2 security.

STEP 3 Under WPS status, choose **Enable**. By default, WPS is disabled.

STEP 4 Click **Save**.

To set up a WPS-enabled device in the network:

STEP 1 Choose **Wireless** > **WPS**.

STEP 2 In the WPS Setup Method section, in the **Station PIN** field, enter the personal identification number (PIN) of the device to connect to the network. You must log in to that device to obtain its WPS PIN.

STEP 3 Click **Configure via PIN** to initiate the WPS session. On the WPS-enabled device, select the necessary option to begin WPS. The device should begin communication with the Cisco RV 120W.

STEP 4 Click **Save**.

Configuring a Wireless Distribution System (WDS)

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 in the WDS. All base stations in a WDS must be configured to use the same radio channel, method of encryption (none, WEP, or WPA) and encryption keys

To configure a WDS:

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

STEP 2 Check the **Enable WDS** box to enable WDS in the Cisco RV 120W.

STEP 3 Enter a WPA password for authentication.

STEP 4 Click **Save**.

You can manually add WDS peers that can connect to the Cisco RV 120W:

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 Cisco RV 120W and includes the following sections:

- Cisco RV 120W Firewall Features, page 74
- Configuring Basic Firewall Settings, page 76
- Configuring Firewall Rules, page 79
- Creating Firewall Schedules, page 85
- Blocking and Filtering Content and Applications, page 85
- Firewall Rule Examples, page 90
- Configuring Port Triggering, page 92
- Configuring Port Forwarding, page 94
- Configuring Remote Management, page 98
- Configuring One-to-One Network Address Translation (NAT), page 99

Cisco RV 120W Firewall Features

You can secure your network by creating and applying rules that the Cisco RV 120W 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 RV 120W, 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:

Protecting from Attacks

Attacks are malicious security breeches or unintentional network issues that render the Cisco RV 120W 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.

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 RV 120W to allow a response to an Internet Control Message Protocol (ICMP) Echo (ping) request on the WAN interface, check this box. This setting is used as a diagnostic tool for connectivity problems. Not enabled by default.
- **Enable 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 will not accept more than 25 simultaneous, active UDP connections from a single computer on the LAN. 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 (UPnP)

UPnP is a feature that allows for automatic discovery of devices that can communicate with the Cisco RV 120W.

To enable UPnP:

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

STEP 2 Check the **Enable** box. If disabled, the Cisco RV 120W does not allow automatic device configuration.

STEP 3 Select the interface 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 RV 120W 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 RV 120W. 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 (i.e. HTTP, FTP, etc.) that the device is using to connect to the Cisco RV 120W.
- **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 RV 120W.

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

Enabling Session Initiation Protocol Application-Level Gateway (SIP ALG)

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 RV 120W.

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 Under the IPv4 or IPv6 fields, 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.

NOTE Ensure that IPv6 support is enabled on the Cisco RV 120W to configure an IPv6 firewall. See **Configuring IPv6, page 54**.

STEP 3 Click **Save.**

Configuring Firewall Rules

All configured firewall rules on the Cisco RV 120W 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.

If you plan to apply a rule to a specific group of devices on your LAN, define the group by selecting **Networking** > **LAN Settings** > **LAN Groups.** See **Configuring LAN Groups, page 45**.

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 85**.
- **Allow by schedule, otherwise block**—Allows the selected type of traffic according to a schedule. See **Creating Firewall Schedules, page 85**.

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 **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 9 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 10 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 11 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) Check the **Enable Port Forwarding** box 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 check the **Enable Port Forwarding** box 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 Address**—Select the public IP address 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 12 Click **Save**.

Managing Firewall Rules

Choose **Firewall** > **Access Control** > **IPv4 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 RV 120W applies rules in the order listed. As a general rule, you should 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** > **Services**.

STEP 2 Enter a service name for identification and management purposes.

STEP 3 Enter the service type, or layer 4 protocol that the service uses (**TCP**, **UDP**, **ICMP**, or **ICMPv6**).

STEP 4 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 5 In the **Start Port** field, enter the first TCP or UDP port of the range that the service uses.

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

STEP 7 Click **Save**.

Creating Firewall Schedules

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

To create a schedule:

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

STEP 2 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 79**.)

STEP 3 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 4 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 5 Click **Save**.

Blocking and Filtering Content and Applications

The Cisco RV 120W 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:

- **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.
- **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.
- **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.

- **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. 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 trusted domain list, then www.yahoo.com will be allowed, but mail.yahoo.com will not be allowed.

NOTE Before adding trusted domains, you must enable content filtering. See **Blocking Web Applications and Components, page 86**.

To add trusted domains:

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

STEP 2 Enter the trusted domain.

STEP 3 Click **Save**.

Adding Blocked Keywords

NOTE Before adding blocked keywords, you must enable content filtering. See **Blocking Web Applications and Components, page 86**.

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

STEP 2 Click **Add**.

STEP 3 Enter the keyword to block. Keywords prevent access to websites that contain the specified characters in the URL or the page contents.

STEP 4 Select the group to which to apply the keyword blocking. (These groups are configured in the **Networking** > **LAN** > **LAN Groups** page.)

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 Check the **Enable** box 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 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 Cisco RV 120W 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 Addresses field, enter the MAC Addresses (the physical address of the piece of hardware) for this rule.

STEP 5 In the IP Addresses field, enter the IP Addresses 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. Logs can be viewed in Status > **View All Logs** page.

Firewall Rule Examples

Example 1: Allow inbound HTTP traffic to the DMZ

In this example, you host a public web server on your local DMZ network. You want to allow inbound HTTP requests from any outside IP address to the IP address of your web server at any time of day.

Create an inbound rule as follows:

Parameter	Value
From Zone	Insecure (WAN1/WAN2)
To Zone	Public (DMZ)
Service	HTTP
Action	Allow always
Send to Local Server (DNAT IP)	192.168.5.2 (web server IP address)
Destination Users	Any
Log	Never

Example 2: Allow videoconferencing from range of outside IP addresses.

In this example, you want to allow incoming videoconferencing to be initiated from a restricted range of outside IP addresses (132.177.88.2 - 132.177.88.254), from a branch office.

Create an inbound rule as follows. In the example, CUSeeMe connections are allowed only from a specified range of external IP addresses.

Parameter	Value
From Zone	Insecure (WAN1/WAN2)
To Zone	Secure (LAN)
Service	CU-SEEME:UDP

Parameter	Value
Action	Allow always
Send to Local Server (DNAT IP)	192.168.1.11
Destination Users	Address Range
From	132.177.88.2
To	134.177.88.254
Enable Port Forwarding	Yes (enabled)

Example 3: Multi-NAT Configuration

In this example, you want to configure multi-NAT to support multiple public IP addresses on one WAN port interface.

Create an inbound rule that configures the firewall to host an additional public IP address. Associate this address with a web server on the DMZ. If you arrange with your ISP to have more than one public IP address for your use, you can use the additional public IP addresses to map to servers on your LAN. One of these public IP addresses is used as the primary IP address of the router. This address is used to provide Internet access to your LAN PCs through NAT. The other addresses are available to map to your DMZ servers.

The following addressing scheme is used to illustrate this procedure:

- WAN IP address: 10.1.0.118
- LAN IP address: 192.168.1.1; subnet 255.255.255.0
- Web server PC in the DMZ, IP address: 192.168.1.2
- Access to Web server: (simulated) public IP address 10.1.0.52

Parameter	Value
From Zone	Insecure (WAN1/WAN2)
To Zone	Public (DMZ)
Service	HTTP
Action	Allow always

Parameter	Value
Send to Local Server (DNAT IP)	192.168.1.2 (local IP address of your web server)
Destination Users	Single Address
From	10.1.0.52
WAN Users	Any
Log	Never

Example 4: Block traffic by schedule if generated from specific range of machines

In this example, you want to block all HTTP traffic on the weekends if the request originates from a specific group of machines in the LAN having a known range of IP addresses, and anyone coming in through the Network from the WAN (i.e. all remote users).

STEP 1 Setup a schedule. Choose **Firewall** > **Access Control** > **Schedules**.

STEP 2 Enter **Weekend** in the Name field.

STEP 3 Under **Scheduled Days**, choose **Specific Days**.

STEP 4 Check the box next to Saturday and Sunday.

STEP 5 Under **Scheduled Time of Day**, select **All Day**. This applies the schedule from 12:00 a.m. to 11:59 p.m. of the selected days.

STEP 6 Click **Save**.

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**.

Configuring Port Forwarding

Port forwarding is used to redirect traffic from the Internet from one port on the WAN to another port on the LAN. The port forwarding rules menu allows selection of a service. Common services are available or you can define a custom service and associated ports to forward.

The Port Forwarding Rules table lists all the available port forwarding rules for this device and allows you to configure port forwarding rules. The table contains the following information:

- **Status**—A port forwarding rule can be disabled if not in use and enabled when needed. The port forwarding rule is disabled if the status is disabled and it is enabled if the status is enabled. Disabling a port forwarding rule does not delete the configuration.
- **Service**—Service for which this port forwarding rule is applicable.
- **Action**—Whether to block or allow traffic (always or by schedule) that meets these filter rules, and when the rule is applicable.
- **Source Users**—The source IP for this port forwarding rule (Any, Single, Range, or Host name).
- **Local Server**—The DNAT IP address, if traffic that meets this filter rule is sent to a local server.
- **Internet Destination**—Which of the WAN ports (if more than one is available) that is the Internet destination for traffic covered by this port forwarding rule.
- **Log**—Whether this port forwarding rule is logged (always or never).

To configure port forwarding:

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

STEP 2 Click **Add**.

STEP 3 Under **Service**, select one of the common or custom services defined for this device:

- 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
- SIP-UDP

STEP 4 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 85**.
- **Allow by schedule, otherwise block**—Allows the selected type of traffic according to a schedule. See **Creating Firewall Schedules, page 85**.

STEP 5 If you selected **block or allow by schedule**, choose the schedule.

STEP 6 Select the **Source Users**:

- **Any**—Specifies that the rule being created is for traffic from the given endpoint.
- **Single Address**—Limit to one host. Requires the IP address of the host to which this rule would be applied.
- **Address Range**—This is used to apply this rule to a group of computers/devices within an IP address range. Requires a **from IP address** and **to IP address**.

STEP 7 If you chose **Single Address** in Step 6, enter the IP address in the field.

STEP 8 If you chose **Address Range** in Step 6, enter the starting IP address of the range in the **From** field and the ending IP address of the range in the **To** field.

STEP 9 Enter the Destination IP address, or the address where traffic meeting the rule should be sent.

STEP 10 In the **Forward to Port** field, choose **Same as Incoming Port** if the traffic should be forwarded to the same port as of the incoming traffic. Choose **Specify Port** if the incoming traffic should be sent to one particular port, and enter the port number to which incoming traffic should be directed.

STEP 11 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**. Enabling logging may generate a significant volume of log messages and is recommended for debugging purposes only. Select **Never** to disable logging.

Restricting Sessions

You can limit the maximum number of unidentified sessions and half-open sessions on the Cisco RV 120W. 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.**

STEP 2 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 3 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 4 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 5 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 6 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 7 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 8 Click **Save**.

Configuring Remote Management

The primary means to configure the Cisco RV 120W is using the browser-based Device Manager. The Device Manager is accessed from a computer on the LAN by using the Cisco RV 120W's LAN IP address and HTTP.

You can enable remote management to allow you to access the Cisco RV 120W from a remote WAN network. To access the Cisco RV 120W remotely, you use HTTP over SSL (https).

To enable remote management:

STEP 1 Check the **Enable** box. By default, remote management is disabled.

CAUTION When remote management is enabled, the router is accessible to anyone who knows its IP address. Since a malicious WAN user can reconfigure the Cisco RV 120W and misuse it in many ways, it is highly recommended that you change the administrator and any guest passwords before continuing. See **Configuring User Accounts, page 127**.

STEP 2 Choose the type of access to grant:

- **All IP Addresses**—Choose to allow any IP address to access the Cisco RV 120W. Change the default password before choosing this option. (See **Configuring User Accounts, page 127**.)

- **IP Address Range**—Choose to allow any IP address in the configured range to access the Cisco RV 120W. 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
- **Only this PC**—Choose to restrict access to only the PC you are currently using to manage the Cisco RV 120W. In the **IP Address** field, enter the IP Address of the PC to be given remote management permissions.

STEP 3 Enter the port number used for the remote connection.

STEP 4 To enable Simple Network Management Protocol (SNMP) to be used remotely to manage the Cisco RV 120W, check the **Remote SNMP Enable** box.

STEP 5 Click **Save**.

Configuring One-to-One Network Address Translation (NAT)

One-to-one 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 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**.

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**.

5

Configuring Virtual Private Networks (VPNs) and Security

This chapter describes VPN configuration, beginning with the **"Configuring VPNs" section on page 102**.

It also describes how to configure router security, beginning with the **"Configuring Security" section on page 115**.

The following sections are covered:

- **Creating Cisco QuickVPN Client Users, page 102**
- **Using the VPN Wizard, page 102**
- **Viewing the Default Values, page 104**
- **Configuring IP Security Policies, page 105**
- **Configuring VPN Policies, page 108**
- **Configuring VPN Clients, page 113**
- **Monitoring VPN Tunnel Status, page 113**
- **Configuring IPsec Users, page 114**
- **Configuring VPN Passthrough, page 115**
- **Using Certificates for Authentication, page 115**
- **Using the Cisco RV 120W With a RADIUS Server, page 118**
- **Configuring 802.1x Port-Based Authentication, page 119**

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 98**.

STEP 2 Create QuickVPN users. See **Configuring IPsec Users, page 114**. 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 for Windows 2000, XP, or Vista."**

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 Set the **Connection Name** and **Pre-Shared** key. The connection name is used for management, and the pre-shared key will be required on the VPN client or gateway to establish the tunnel.

STEP 3 Choose the Remote Gateway Type (**IP Address** or **Fully-Qualified Domain Name**).

STEP 4 Enter the Remote WAN IP Address/Internet Name.

STEP 5 Choose the Local Gateway Type (**IP Address** or **Fully-Qualified Domain Name**).

STEP 6 Enter the Local WAN IP Address/Internet Name. 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 7 Configure the LAN accessibility details in the Secure Connection Remote Accessibility section:

- Remote LAN IP address
- Remote LAN Subnet Mask

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

STEP 8 Click **Save**.

STEP 9 The Wizard creates a corresponding IKE policy with the following default values (these can be accessed from a link on the Wizard page):

Parameter	Default value from Wizard
Exchange Mode	Aggressive
ID Type	FQDN
Local WAN ID	wan_local.com
Remote WAN ID	wan_remote.com
Encryption Algorithm	3DES
Authentication Algorithm	SHA-1
Authentication Method	Pre-shared Key
Key-Group	DH-Group 2(1024 bit)
Life Time	24 hours

The Wizard creates a corresponding VPN policy with the following default values:

Parameter	Default value from Wizard
Encryption Algorithm	3DES
Authentication Algorithm	SHA-1
Life Time	8 hours
PFS Key Group	DH-Group 2(1024 bit)
NETBIOS	Enabled

Viewing the Default Values

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

Configuring IP Security Policies

The VPN Wizard is the recommended method to configure corresponding 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 Internet Key Exchange (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 mode**—This mode negotiates the tunnel with higher security, but is slower.
- **Aggressive mode**—This mode establishes a faster connection, but with lowered security.

NOTE If either the Local or Remote identifier type 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**
- **Internet Address/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:

- **Local WAN IP**
- **Internet Address/FQDN**
- **User FQDN**
- **DER ASN1 DN**

STEP 7 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.

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 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 114**.

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**—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**—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 **Enable NetBIOS** field, check this box 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 user name, 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 **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 Cisco RV 120W, 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 Security

The Cisco RV 120W provides several security methods, including certificate authentication, RADIUS server support, and 802.1x port-based authentication.

Using Certificates for Authentication

The Cisco RV 120W 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-signed 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-signed) 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-signed 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 on the View button next to the appropriate request in this table.

Downloading the Router's Current Certificate

To download the router's current certificate, under **Download Settings**, 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 RV 120W 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 Cisco RV 120W re-authenticates with the RADIUS server.
- Retries: The number of retries for the Cisco RV 120W 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 Cisco RV 120W 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 Cisco RV 120W re-authenticates with the RADIUS server.

STEP 6 In the **Retries** field, enter the number of retries for the Cisco RV 120W 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 Cisco RV 120W 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 Cisco RV 120W 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 (QoS)

The Cisco RV 120W provides configuration for QoS features, such as bandwidth profiles, traffic selectors, and traffic meters. It contains the following sections:

- Configuring Bandwidth Profiles, page 120
- Configuring Traffic Flows, page 121
- Configuring Traffic Metering, page 122
- Configuring 802.1p, page 124

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 Flows

After a profile has been created, it can then be associated with a traffic flow. 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 120**.)

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 84**.)

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 type of action to be taken on the traffic counter:

- **Restart Counter Now**—Select this option and click **Save** to reset the counter to zero immediately.
- **Restart Traffic Counter at 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.
- **Send E-mail Report before restarting counter**—Select this option to receive an e-mail report before the traffic counter is restarted. The e-mail will be sent to the address configured in the Logging section.

NOTE This feature works only if you enable e-mail logs on the **Administration** > **Logging** > **Remote Logging** page. See **Configuring Logging, page 131**.

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:

- **Send e-mail alert**—Check this option to send an e-mail when traffic limit is reached.
- **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. This feature works only if you enable e-mail logs on the **Administration** > **Logging** > **Remote Logging** page. See **Configuring Logging, page 131**.

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**.

7

Administering Your Cisco RV 120W

This chapter describes the administration features of the Cisco RV 120W, including creating users, configuring network management, diagnostics and logging, date and time, and other settings. It contains the following sections:

- Setting Password Complexity, page 126
- Configuring User Accounts, page 127
- Setting the Timeout Value, page 128
- Configuring Simple Network Management (SNMP), page 128
- Using Diagnostic Tools, page 130
- Configuring Logging, page 131
- Configuring Discovery (Bonjour), page 135
- Configuring Date and Time Settings, page 136
- Backing Up and Restoring the System, page 137
- Upgrading Firmware, page 138
- Rebooting the Cisco RV 120W, page 138
- Restoring the Factory Defaults, page 138

Setting Password Complexity

The Cisco RV 120W 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 contains characters from at least 3 of the following 4 categories:
  - Uppercase letters
  - Lowercase letters
  - Numbers
  - Special characters available on a standard keyboard.
- Passwords cannot be the same as the username, which is “admin” by default.
- New passwords cannot be the same as the current password.

Configuring User Accounts

The Cisco RV 120W supports two user accounts for administering and viewing settings: an administrative user (default user name: “admin”) and a “guest” user (default user name: “guest”). The guest account has read-only access. You can set and change the username and password for both the administrator and guest accounts.

To configure the user accounts:

STEP 1 Choose **Administration** > **Users**.

STEP 2 Click the button to edit either the **Admin** or **User** account.

STEP 3 Enter the new username.

STEP 4 Enter the old password.

STEP 5 Enter the new password. It is recommended that passwords contains no dictionary words from any language, and are a mix of letters (both uppercase and lowercase), numbers, and symbols. The password can be up to 30 characters.

STEP 6 Click **Save**.

Setting the Timeout Value

The timeout value is the number of minutes of inactivity that are allowed before the Device Manager session is ended. This can be configured for the Admin and Guest accounts:

STEP 1 Choose **Administration** > **Session Timeout**.

STEP 2 Enter the number, in minutes, before a session times out due to inactivity.

STEP 3 Click **Save**.

Configuring Simple Network Management (SNMP)

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 Cisco RV 120W user accounts (Admin and Guest). To configure:

STEP 1 In the **SNMPv3 Users List Table**, check the box for the user to edit and click **Edit**.

STEP 2 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 3 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 4 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**—Enter a name for easy identification of the router.

STEP 2 Click **Save.**

Using Diagnostic Tools

The Cisco RV 120W provides several diagnostic tools. To access these tools, choose **Administration** > **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.

Using Trace Route

This utility will display all the routers present between the destination IP address and this router. 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 Cisco RV 120W 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, etc. 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** or **IPv6 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** or **IPv6 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** > **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 Discovery (Bonjour)

Bonjour is a service advertisement and discovery protocol. For the Cisco RV 120W, Bonjour only advertises the default services configured on the device when Bonjour is enabled.

To configure 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.

Currently the services **csco-sb** and **http** are available and active by default. When remote management is enabled, **https** service is enabled and advertised. (See **Configuring Remote Management, page 98**.)

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 Virtual LANs (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 Virtual LANs (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 the **Adjust for Daylight Savings Time** box.

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.

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.

You can upgrade to a newer software version from the **Administration** > **Firmware Upgrade** page. To upgrade:

In the Router Upgrade screen area, click **Browse**, locate and select the downloaded firmware, and click **Upload**.

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 RV 120W

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**.

A

Using Cisco QuickVPN for Windows 2000, XP, or Vista

Overview

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

This appendix includes the following sections:

- **Before You Begin, page 139**
- **Installing the Cisco QuickVPN Software, page 140**
- **Using the Cisco QuickVPN Software, page 142**
- **, page 145**

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 98**.

STEP 2 Create Quick VPN user accounts. See **Configuring IPsec Users, page 114**. After a user account is created, the credentials can be used by the Quick VPN client.

Installing the Cisco QuickVPN Software

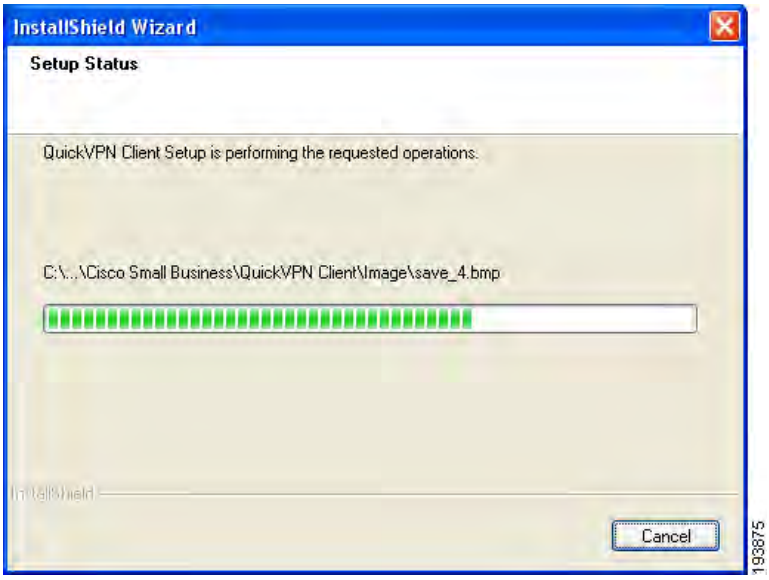
Installing from the CD-ROM

STEP 1 Insert the Cisco RV 120W CD-ROM into your CD-ROM drive. After the Setup Wizard begins, click the **Install QuickVPN** link.

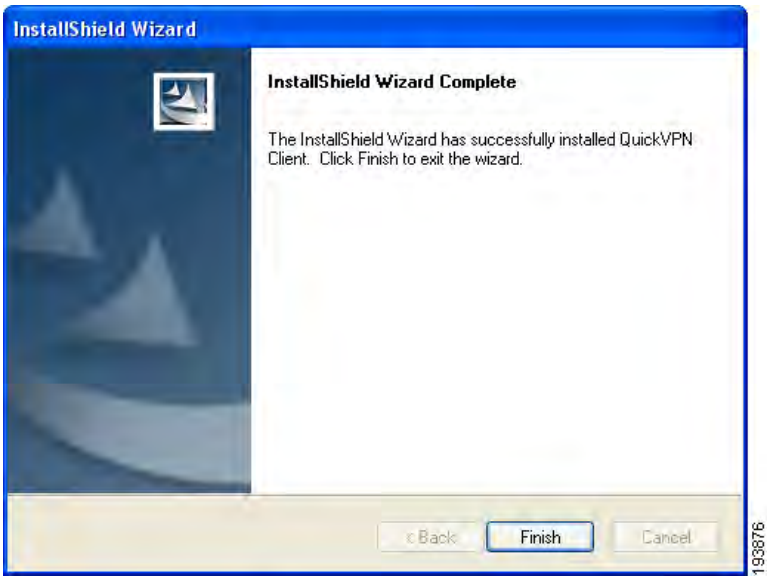
STEP 2 The License Agreement window appears. Click **Yes** to accept the agreement and the appropriate files are copied to the computer.

License Agreement

Copying Files



Finished Installing Files



STEP 3 Click **Finished** to complete the installation. Proceed to **"Using the Cisco QuickVPN Software," on page 142**.

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 RV 120W 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 142**.

Using the Cisco QuickVPN Software

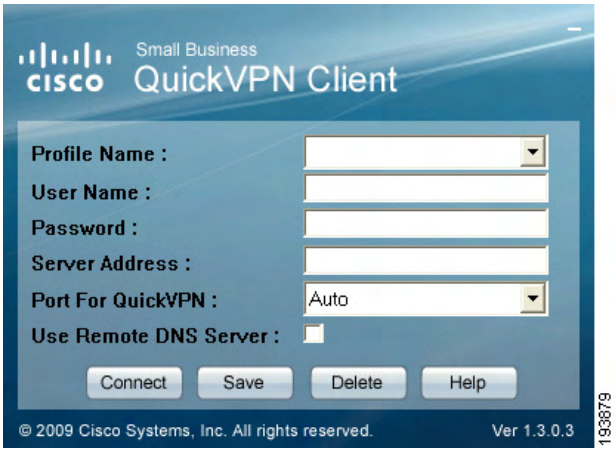
STEP 1 Double-click the Cisco QuickVPN software icon on your desktop or in the system tray.

QuickVPN Desktop Icon

QuickVPN Tray Icon—
No Connection

STEP 2 The QuickVPN Login window will appear. 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 114**. In the **Server Address** field, enter the IP address or domain name of the Cisco RV 120W. In the **Port For QuickVPN** field, enter the port number that the QuickVPN client will use to communicate with the remote VPN router, or keep the default setting, **Auto**.

QuickVPN Login



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

STEP 3 To begin your QuickVPN connection, click **Connect**. The connection's progress is displayed: *Connecting*, *Provisioning*, *Activating Policy*, and *Verifying Network*.

STEP 4 When your QuickVPN connection is established, the QuickVPN tray icon turns green, and the QuickVPN Status window appears. The window displays the IP address of the remote end of the VPN tunnel, the time and date the VPN tunnel began, and the total length of time the VPN tunnel has been active.

QuickVPN Tray Icon—Connection

QuickVPN Status

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

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

Connect Virtual Private Connection

NOTE You can change your password only if the **Allow User to Change Password** box has been checked for that username. See **Configuring IPsec Users, page 114**.

B

Where to Go From Here

Cisco provides a wide range of resources to help you obtain the full benefits of the Cisco RV 120W.

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 RV 120W	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