



ADMINISTRATION GUIDE

Cisco Small Business

RV120W Wireless-N VPN Firewall

Revised June 2011

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Chapter 1: Introduction	1
Product Overview	1
LAN Ethernet Interfaces	2
Wireless Access Point	2
Firewall and VPN Client Access	2
Wireless Distribution System	2
Virtual Networks	2
Security	3
Quality of Service	3
Configuration and Administration	3
Getting to Know the Cisco RV120W	4
Front Panel	4
Back Panel	5
Mounting the Cisco RV120W	6
Installation Guidelines	6
Wall Mounting	6
Connecting the Equipment	8
Setting Up the Cisco RV120W Using the Setup Wizard	12
Using the Getting Started Page	13
Initial Settings	14
Quick Access	14
Device Status	15
Other Resources	15
Navigating through the Pages	15
Saving Your Changes	17
Viewing the Help Files	18
Connecting Devices to Your Wireless Network	18
	18

Chapter 2: Configuring Networking	19
Configuring the WAN (Internet) Settings	19
Configuring the IPv4 WAN (Internet)	20
Configuring Automatic Configuration (DHCP)	20
Configuring Static IP	21
Configuring PPPoE	21
Configuring PPTP	22
Configuring L2TP	23
Configuring MTU Settings	24
Configuring the MAC Address	24
Configuring PPPoE Profiles	25
Configuring the LAN (Local Network) Settings	27
Configuring IPv4 LAN (Local Network) Settings	27
Configuring the Host Name	27
Configuring the IP Address	27
Configuring DHCP	28
Configuring the DNS Proxy	29
Configuring Virtual LAN (VLAN) Membership	30
Enabling VLANs	30
Creating a VLAN	30
Configuring Multiple VLAN Subnets	31
Configuring Static DHCP	32
Configuring Advanced DHCP Settings	33
Configuring Automatic Configuration Download	33
Adding a DHCP Client to Configuration File Map	34
Viewing DHCP Leased Clients	34
Configuring Routing	34
Choosing the Routing Mode	34
Viewing Routing Information	35
Configuring Static Routes	37
Configuring Dynamic Routing	38
Configuring Port Management	40
Configuring Dynamic DNS (DDNS)	40

Configuring IPv6	42
Configuring the IP Mode	42
Configuring IPv6 WAN Settings	42
Configuring DHCPv6	42
Configuring a Static IP Address	43
Configuring IPv6 LAN Properties	43
Configuring IPv6 Address Pools	45
Configuring IPv6 Routing	45
Configuring Dynamic Routing	45
Configuring Static Routing	46
Configuring Tunneling	47
Viewing IPv6 Tunnel Information	47
Configuring Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) Tunnels	48
Configuring Router Advertisement	49
Configuring Router Advertisement Prefixes	50

Chapter 3: Configuring the Wireless Network51

A Note About Wireless Security	51
Wireless Security Tips	52
General Network Security Guidelines	53
Understanding the Cisco RV120W's Wireless Networks	54
Configuring Basic Wireless Settings	54
Configuring Radio, Mode, and Channel Settings	54
Configuring Wireless Security and Other Settings	55
Configuring Security	56
Configuring MAC Filtering	58
Configuring Wi-Fi Multimedia	59
Configuring Wireless Network (SSID) Scheduling	60
Configuring Advanced Wireless Settings	61
Configuring Wi-Fi Protected Setup	62
Configuring a Wireless Distribution System (WDS)	63

Chapter 4: Configuring the Firewall	65
Cisco RV120W Firewall Features	65
Configuring Access Rules	67
Configuring the Default Outbound Policy	67
Creating an Access Rule	67
Configuring Attack Prevention	71
Configuring Content Filtering	72
Enabling Content Filtering	72
Blocking Web Components	73
Adding Trusted Domains	74
Configuring URL Blocking	74
Configuring Port Triggering	75
Configuring Port Forwarding	76
Configuring a DMZ Host	80
Configuring Advanced Firewall Settings	80
Configuring One-to-One Network Address Translation (NAT)	80
Configuring MAC Address Filtering	81
Configuring IP/MAC Address Binding	82
Creating Custom Services	83
Creating Firewall Schedules	84
Configuring Sessions	84
Configuring Internet Group Management Protocol (IGMP)	85
Configuring LAN (Local Network) Groups	86
Enabling Session Initiation Protocol Application-Level Gateway (SIP ALG)	87
Firewall Configuration Examples	87
Chapter 5: Configuring Virtual Private Networks (VPNs) and Security	92
Configuring VPNs	92
Creating Cisco QuickVPN Client Users	93

Configuring a Basic VPN	93
Viewing the Default VPN Settings	94
Configuring Advanced VPN Parameters	94
Configuring IKE Policies	95
Configuring VPN Policies	98
Configuring VPN Clients	103
Monitoring VPN Tunnel Status	104
Configuring VPN Users	105
Configuring a PPTP Server	105
Adding New VPN Users	106
Configuring VPN Passthrough	106
Configuring Security	107
Using Certificates for Authentication	107
Generating New Certificates	108
Importing a Certificate from a File	108
Exporting the Router's Current Certificate	109
Using the Cisco RV120W With a RADIUS Server	109
Configuring 802.1x Port-Based Authentication	110
Chapter 6: Configuring Quality of Service (QoS)	112
Configuring WAN QoS Profiles	112
Configuring Profile Binding	114
Configuring CoS Settings	115
Mapping CoS Settings to DSCP Values	116
Chapter 7: Administering Your Cisco RV120W	117
Configuring Password Rules	118
Using the Management Interface	118
Configuring Web Access	119
Configuring Remote Management	119
Configuring User Accounts	120
Setting the Session Timeout Value	120

Configuring Network Management	121
Configuring SNMP	121
Editing SNMPv3 Users	121
Adding SNMP Traps	122
Configuring Access Control Rules	122
Configuring Additional SNMP Information	123
Configuring the WAN Traffic Meter	123
Using Network Diagnostic Tools	125
Using PING	125
Using Traceroute	125
Performing a DNS Lookup	126
Capturing and Tracing Packets	126
Configuring Logging	126
Configuring Logging Policies	127
Configuring Firewall Logs	127
Configuring Remote Logging	128
Configuring Email Logging	129
Configuring the Discovery Settings	130
Configuring Bonjour	130
Configuring UPnP	131
Configuring Time Settings	132
Backing Up and Restoring the System	132
Upgrading Firmware	134
Rebooting the Cisco RV120W	134
Restoring the Factory Defaults	135
Chapter 8: Viewing the Cisco RV120W Status	136
Viewing the Dashboard	136
Viewing the System Summary	139
Viewing the Wireless Statistics	142
IPsec Connection Status	143
Viewing VPN Client Connection Status	144

Viewing Logs	145
Viewing Available LAN Hosts	146
Viewing Port Triggering Status	147
Viewing Port Statistics	148
Viewing Open Ports	149
Appendix A: Using Cisco QuickVPN for Windows 7, 2000, XP, or Vista	150
Overview	150
Before You Begin	150
Installing the Cisco QuickVPN Software	151
Installing from the CD-ROM	151
Downloading and Installing from the Internet	151
Using the Cisco QuickVPN Software	152
Appendix B: Where to Go From Here	154

Introduction

This chapter describes the features of the Cisco RV120W, guides you through the installation process, and gets you started using the Device Manager, a browser-based utility for configuring the Cisco RV120W.

- [Product Overview, page 1](#)
- [Getting to Know the Cisco RV120W, page 4](#)
- [Mounting the Cisco RV120W, page 6](#)
- [Connecting the Equipment, page 8](#)
- [Setting Up the Cisco RV120W Using the Setup Wizard, page 12](#)
- [Using the Getting Started Page, page 13](#)
- [Navigating through the Pages, page 15](#)
- [Saving Your Changes, page 17](#)
- [Viewing the Help Files, page 18](#)
- [Connecting Devices to Your Wireless Network, page 18](#)

Product Overview

Thank you for choosing the Cisco Small Business RV120W Wireless-N VPN Firewall.

The Cisco RV120W 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 RV120W 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.

LAN Ethernet Interfaces

The Cisco RV120W provides four full-duplex 10/100 Ethernet LAN interfaces that can connect up to four devices.

Wireless Access Point

The wireless access point supports the 802.11n standard with MIMO technology, which multiplies the effective data rate. This technology provides better throughput and coverage than 802.11g networks.

Firewall and VPN Client Access

The Cisco RV120W 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 RV120W 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

Wireless Distribution System

The Cisco RV120W's wireless access point supports Wireless Distribution System (WDS), which allows the wireless coverage to be expanded without wires.

Virtual Networks

The access point 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.

Security

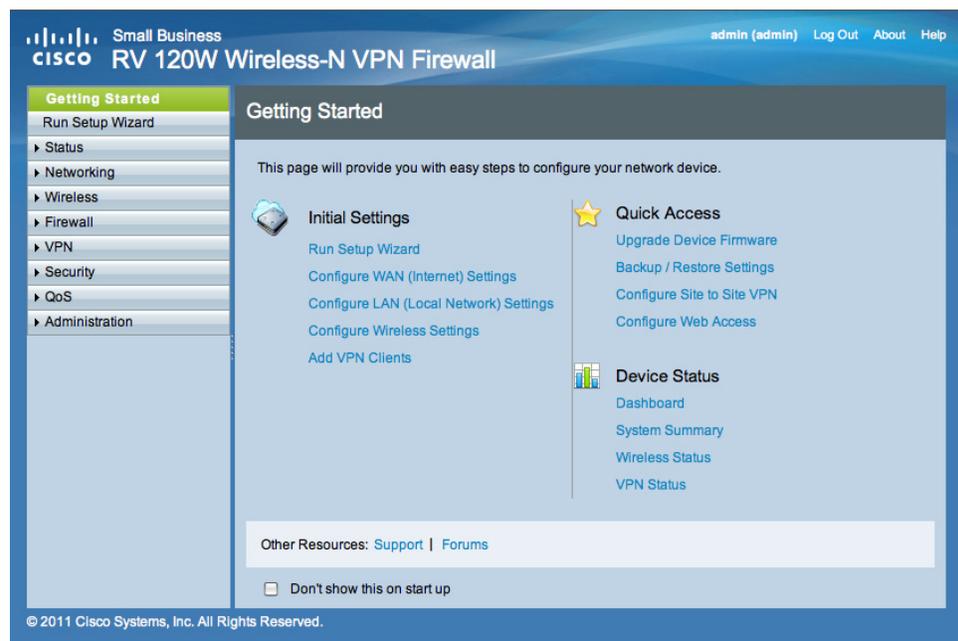
The Cisco RV120W implements WPA2-PSK, WPA2-ENT, and WEP encryption, along with other security features including the disabling of SSID broadcasts, MAC-based filtering, and allowing or denying “time of day” access per SSID.

Quality of Service

The Cisco RV120W 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.

Configuration and Administration

With the Cisco RV120W’s embedded web server, you can configure the firewall’s settings using the browser-based Device Manager. The Cisco RV120W supports Internet Explorer, Firefox, and Safari web browsers.



The Cisco RV120W also provides a setup wizard. The setup wizard allows you to easily configure the Cisco RV120W's basic settings.

Getting to Know the Cisco RV120W

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 RV120W. If the LED is continuously lit green, the Cisco RV120W is connected to a device through the corresponding port (1, 2, 3, or 4). The LED for a port flashes green when the Cisco RV120W is actively sending or receiving data over that port.

Back Panel



RESET Button—The Reset button has two functions:

- If the Cisco RV120W 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 RV120W 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 RV120W 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 RV120W 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 RV120W

You can place your Cisco RV120W 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.

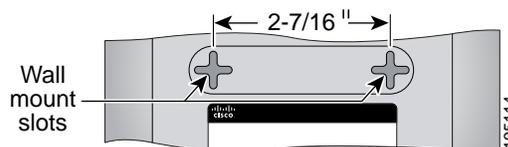
For desktop placement, place the Cisco RV120W device horizontally on a flat surface so that it sits on its four rubber feet.

Wall Mounting

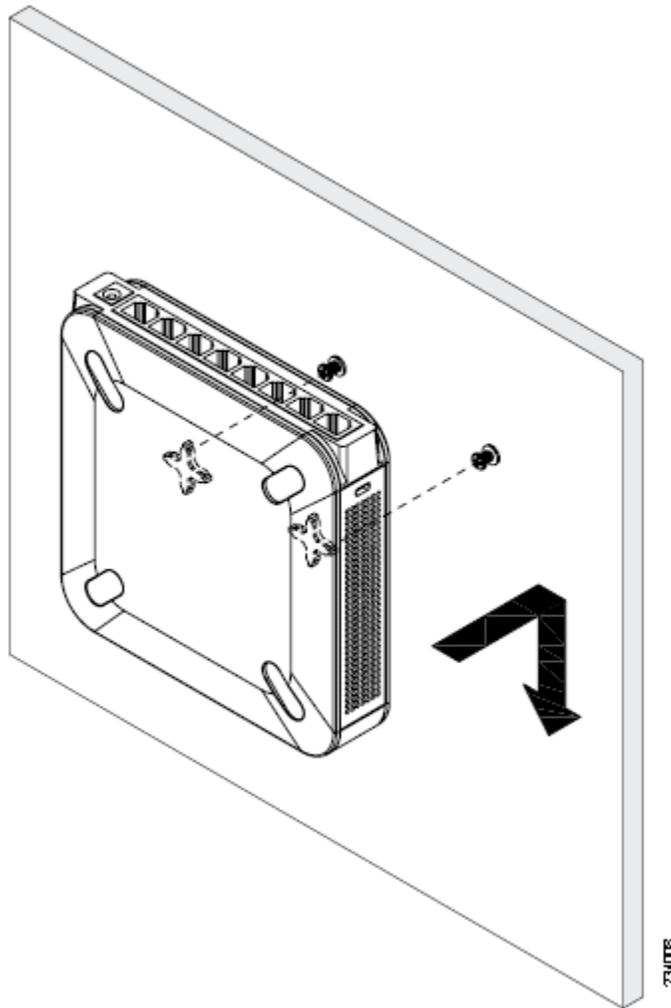
- STEP 1** Determine where you want to mount the device and install two screws (not supplied) that are 2-7/16 in. apart (approximately 61 mm). Mounting screws should have a head that is approximately 5.5 mm in diameter and 2 mm deep, with a shaft that is at least 15.5 mm long and approximately 3.5 mm 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. 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 firewall to a PC for configuration.

Optional

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

To connect your firewall to the Internet:

- STEP 1** Power off all equipment, including the cable or DSL modem, the PC you will use to connect to the RV120W, and the RV120W.
- STEP 2** Use an Ethernet cable to connect the WAN port of the Cisco RV120W to your cable or DSL modem.



- STEP 3** Connect one end of a different Ethernet cable to one of the LAN (Ethernet) ports on the back of the RV120W. (In this example, the LAN 2 port is used.) Connect the other end of the cable to an Ethernet port on the PC.



- STEP 4** Power on the cable or DSL modem and wait until the connection is active.

STEP 5 Connect the power adapter to the Cisco RV120W power port (12VDC).



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



STEP 6 Plug the other end of the adapter into an electrical outlet. You may need to use a specific plug (supplied) for your country.

STEP 7 On the Cisco RV120W, push in the ON/OFF power button.



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

Setting Up the Cisco RV120W Using the Setup Wizard

With the RV120W powered on and connected to a PC, use the Setup Wizard to configure the Cisco RV120W.

To use the Setup Wizard:

STEP 1 Start the PC connected to the RV120W.

Your computer becomes a DHCP client of the RV120W and receives an IP address in the 192.168.1.xxx range.

STEP 2 Launch a web browser and enter **192.168.1.1** in the **Address** field.

This is the default IP address of the RV120W.

STEP 3 When the login page appears, enter the user name and password.

The default user name is **admin**. The default password is **admin**. The password is case sensitive.

STEP 4 Click **Log In**.

The Setup Wizard starts.

STEP 5 Follow the Setup Wizard's on-screen instructions to set up the RV120W.

The Setup Wizard tries to automatically detect and configure your connection. If it cannot, the Setup Wizard asks you for information about your Internet connection. If you do not have it, contact your Internet Service Provider (ISP) to obtain this information.

During the setup process, the Setup Wizard asks you to enter a new password. To protect your firewall from unauthorized access, create a new password that is hard to figure out by others. While you are entering the password, the Setup Wizard provides you with instant feedback regarding the strength of the password.

After the Setup Wizard is done configuring the RV120W, the **Getting Started** page appears. See [Using the Getting Started Page, page 13](#) for more information.

Using the Getting Started Page

The **Getting Started** page displays the most common Cisco RV120W configuration tasks. Use the links on this page to jump to the relevant configuration page.

By default, this page appears when you start the Device Manager. However, you can change this behavior by checking **Don't show this on start up** at the bottom of the page.

Initial Settings

Run Setup Wizard	Click this link to launch the Setup Wizard.
Configure WAN (Internet) Settings	Click this link to open the Internet Setup page. See Configuring the IPv4 WAN (Internet) , page 20.
Configure LAN (Local Network) Settings	Click this link to open the LAN Configuration page. See Configuring IPv4 LAN (Local Network) Settings , page 27.
Configure Wireless Settings	Click this link to open the Basic Settings page. See Configuring Basic Wireless Settings , page 54.
Add VPN Clients	See Configuring VPN Users , page 105.

Quick Access

Upgrade Device Firmware	Click this link to open the Firmware Upgrade page. See Upgrading Firmware , page 134.
Backup/Restore Settings	Click this link to open the Backup and Restore page. See Backing Up and Restoring the System , page 132
Configure Site to Site VPN	Click this link to open the Basic VPN Setup page. See Configuring a Basic VPN , page 93.
Configure Web Access	Click this link to open the Web Access page. See Configuring Web Access , page 119.

Device Status

Dashboard	Click this link to open the Dashboard page. See Viewing the Dashboard, page 136 .
System Summary	Click this link to open the System Summary page. See Viewing the System Summary, page 139 .
Wireless Status	Click this link to open the Wireless Statistics page. See Viewing the Wireless Statistics, page 142 .
VPN Status	Click this link to open the IPsec Connection Status page. See IPsec Connection Status, page 143 .

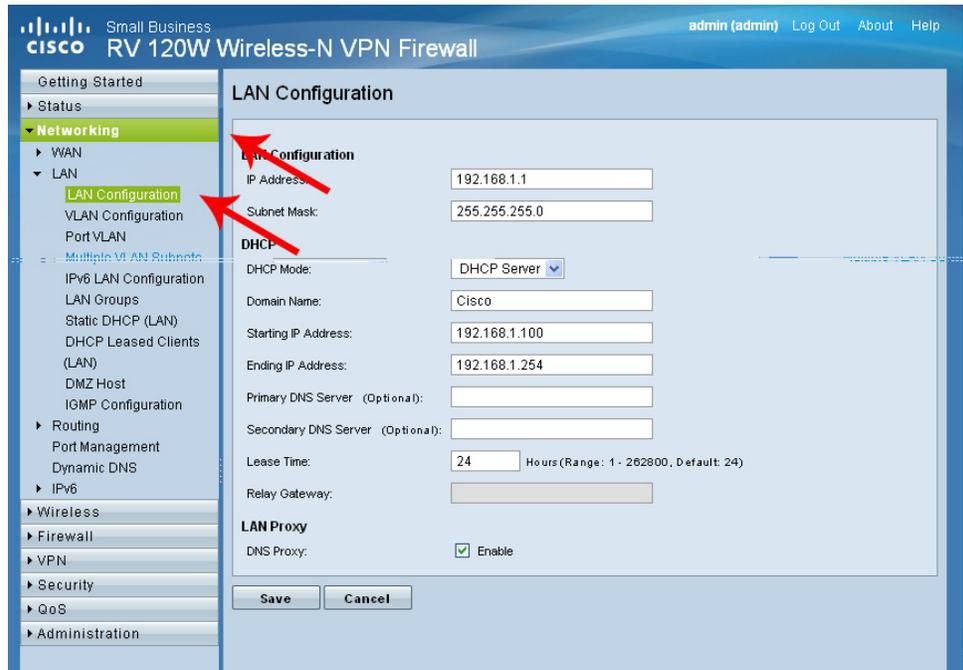
Other Resources

Support	Click this link to open Cisco's support page.
Forums	Click this link to visit Cisco's online support forums.

Navigating through the Pages

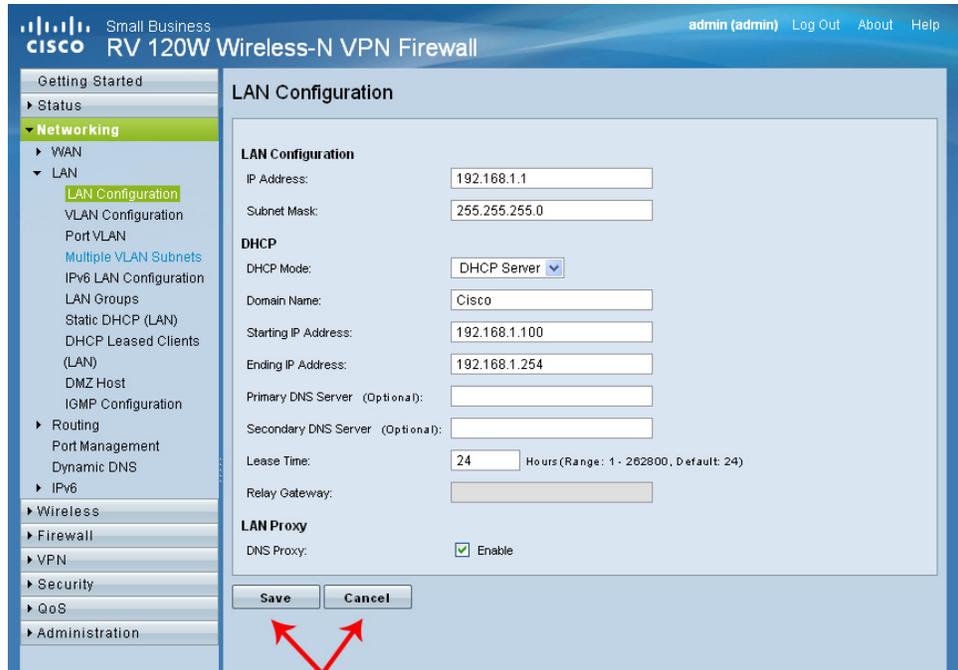
Use the navigation tree in the left pane to open the configuration pages.

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.



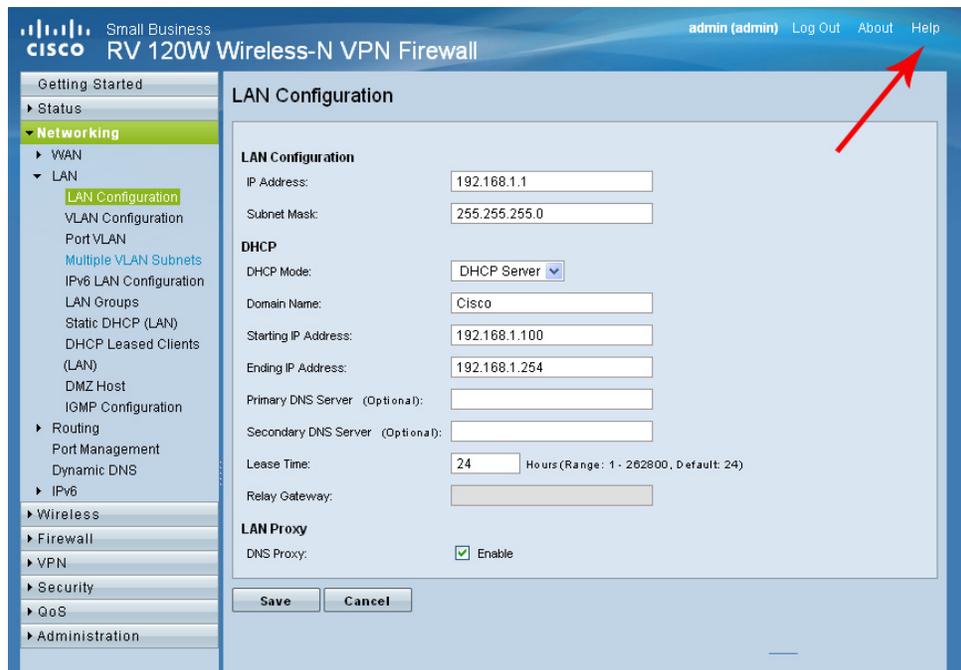
Saving Your Changes

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.



Connecting Devices to Your Wireless Network

To connect a device such as a PC or printer to your wireless network, you must configure the wireless connection on the device using the security information you configured for the Cisco RV120W:

- Network name or Service Set Identifier (SSID). The default SSID is ciscosb-1.
- If applicable, the encryption type and security key.

Configuring Networking

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

- [Configuring the WAN \(Internet\) Settings, page 19](#)
- [Configuring the LAN \(Local Network\) Settings, page 27](#)
- [Configuring Routing, page 34](#)
- [Configuring Port Management, page 40](#)
- [Configuring Dynamic DNS \(DDNS\), page 40](#)
- [Configuring IPv6, page 42](#)

**NOTE**

Cisco recommends you use the Setup Wizard to configure basic networking on the Cisco RV120W. You can then make changes and provision advanced features using the Device Manager.

Configuring the WAN (Internet) Settings

If you have an IPv4 network, use these sections to configure your network. If you have an IPv6 network, see [Configuring IPv6, page 42](#).

Configuring the IPv4 WAN (Internet)

-
- STEP 1** Choose **Networking > WAN (Internet) > IPv4 WAN (Internet)**.
- STEP 2** Choose the type of Internet connection you have. The type of connection you have determines the rest of the information you need to enter. See the sections below for more information:
- [Configuring Automatic Configuration \(DHCP\), page 20](#)
 - [Configuring Static IP, page 21](#)
 - [Configuring PPPoE, page 21](#)
 - [Configuring PPTP, page 22](#)
 - [Configuring L2TP, page 23](#)
-

Configuring Automatic Configuration (DHCP)

If your Internet Service Provider (ISP) uses the Dynamic Host Configuration Protocol (DHCP) to assign you an IP address, you receive a dynamic IP address from your ISP.

To configure DHCP WAN settings:

-
- STEP 1** Choose **Networking > WAN (Internet) > IPv4 WAN (Internet)**.
- STEP 2** From the **Internet Connection Type** drop-down menu, choose **Automatic Configuration - DHCP**.
- STEP 3** Enter MTU information. (See [Configuring MTU Settings, page 24.](#))
- STEP 4** Enter MAC Address information. (See [Configuring the MAC Address, page 24.](#))
- STEP 5** Click **Save**.
-

Configuring Static IP

If your ISP assigned you a permanent IP address, perform the following steps to configure your WAN settings:

-
- STEP 1** Choose **Networking > WAN (Internet) > IPv4 WAN (Internet)**.
- STEP 2** From the **Internet Connection Type** drop-down menu, choose **Static IP**.
- STEP 3** Enter this information:

IP Address	Enter the IP address of the WAN port.
Subnet mask	Enter subnet mask of the WAN port.
Default Gateway	Enter the IP address of the default gateway.
Primary DNS Server	Enter the IP address of the primary DNS server.
Secondary DNS Server	(Optional) Enter the IP address of the secondary DNS server.

- STEP 4** Enter MTU information. (See [Configuring MTU Settings, page 24.](#))
- STEP 5** Enter MAC Address information. (See [Configuring the MAC Address, page 24.](#))
- STEP 6** Click **Save**.
-

Configuring PPPoE

If you have a Point-to-Point Protocol over Ethernet (PPPoE) connection to the Internet:

-
- STEP 1** Choose **Networking > WAN (Internet) > IPv4 WAN (Internet)**.
- STEP 2** From the **Internet Connection Type** drop-down menu, choose **PPPoE**.
- STEP 3** From the **PPPoE Profile Name** drop-down menu, choose a PPPoE profile.

If no profile is listed, click **Configure Profile** to create a new profile.

To see the details of available profiles, choose **Networking > WAN (Internet) > PPPoE Profiles**. See [Configuring PPPoE Profiles, page 25](#) for more information.

- STEP 4** Enter MTU information. (See [Configuring MTU Settings, page 24.](#))

STEP 5 Enter MAC Address information. (See [Configuring the MAC Address, page 24.](#))

STEP 6 Click **Save**.

Configuring PPTP

If you have a Point-to-Point Tunneling Protocol (PPTP) connection to the Internet:

STEP 1 Choose **Networking > WAN (Internet) > IPv4 WAN (Internet)**.

STEP 2 From the **Internet Connection Type** drop-down menu, choose **PPTP**.

STEP 3 Enter this information:

User Name	Enter your username assigned to you by the ISP.
Password	Enter your password assigned to you by the ISP.
MPPE Encryption	If your ISP supports Microsoft Point-to-Point Encryption (MPPE), check to enable MPPE encryption.
Connection Type	Choose the connection type: <ul style="list-style-type: none"> ▪ 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 option if your ISP charges based on connection time.
Idle Time	If you choose Idle Time as the connection type, enter the number of minutes after which the connection terminates. The valid range is 5–999 .
My IP Address	Enter the IP address assigned to you by your ISP.
Server IP Address	Enter the IP address of the PPTP server.

STEP 4 Enter MTU information. (See [Configuring MTU Settings, page 24.](#))

STEP 5 Enter MAC Address information. (See [Configuring the MAC Address, page 24.](#))

STEP 6 Click **Save**.

Configuring L2TP

If you have a Layer 2 Tunneling Protocol (L2TP) connection to the Internet:

STEP 1 Choose **Networking > WAN**.

STEP 2 From the **Internet Connection Type** drop-down menu, choose **L2TP**.

STEP 3 Enter this information:

User Name	Enter your username assigned to you by the ISP.
Password	Enter your password assigned to you by the ISP.
Secret	(Optional) Enter your secret phrase. This phrase is known to you and your ISP for use in authenticating your logon.
Connection Type	Choose the connection type: <ul style="list-style-type: none"> ▪ 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 option if your ISP charges based on connection time.
Idle Time	If you choose Idle Time as the connection type, enter the number of minutes after which the connection terminates. The valid range is 5–999 .
My IP Address	Enter the IP address assigned to you by your ISP.
Server IP Address	Enter the IP address of the L2TP server.

STEP 4 Enter MTU information. (See [Configuring MTU Settings, page 24.](#))

STEP 5 Enter MAC Address information. (See [Configuring the MAC Address, page 24.](#))

STEP 6 Click **Save**.

Configuring MTU Settings

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

To configure the MTU settings:

STEP 1 Choose **Networking** > Choose **Networking** > **WAN (Internet)** > **IPv4 WAN (Internet)**.

STEP 2 Choose the MTU type:

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

STEP 3 Click **Save**.

Configuring the MAC Address

The Cisco RV120W has a unique 48-bit local Ethernet hardware address. In most cases, the default MAC address is used to identify your Cisco RV120W to your ISP. However, you can change this setting if required by your ISP.

To configure the MAC address settings:

STEP 1 Choose **Networking > WAN (Internet) > IPv4 WAN (Internet)**.

STEP 2 From the **Router MAC Address** drop-down menu, choose one of these options:

- **Use Default Address**—(Recommended) choose this option to use the default MAC address.
- **Use This Computer's Address**—Choose this option to assign the MAC address of your computer.
- **Use This MAC**—Choose this option if you want to use the MAC address of the PC on which you are connecting to the Device Manager.

STEP 3 Click **Save**.

Configuring PPPoE Profiles

If you have a PPPoE connection to the Internet, you can create profiles for multiple PPPoE accounts. This can be useful if you connect to the Internet using different service provider accounts.

STEP 1 Choose **Networking > WAN (Internet) > PPPoE Profiles**.

STEP 2 Click **Add** to create a new profile.

STEP 3 Enter the following information (you may need to contact your ISP to obtain your PPPoE login information):

Profile Name	Enter the name of the profile.
Username	Enter your username assigned to you by the ISP.
Password	Enter your password assigned to you by the ISP.

<p>Authentication Type</p>	<p>Choose the authentication type from the drop-down menu:</p> <p>Auto-negotiate—The server sends a configuration request specifying the security algorithm set on it. Then, the Cisco RV120W sends back authentication credentials with the security type sent earlier by the server.</p> <p>PAP—The Cisco RV120W uses the Password Authentication Protocol (PAP) to connect to the ISP.</p> <p>CHAP—The Cisco RV120W uses the Challenge Handshake Authentication Protocol (CHAP) when connecting with the ISP.</p> <p>MS-CHAP or MS-CHAPv2—The Cisco RV120W uses Microsoft Challenge Handshake Authentication Protocol when connecting with the ISP.</p>
<p>Connection Type</p>	<p>Choose the connection type:</p> <ul style="list-style-type: none"> ▪ 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 option if your ISP charges based on connection time.
<p>Idle Time</p>	<p>If you choose Idle Time as the connection type, enter the number of minutes after which the connection terminates. The valid range is 5–999.</p>

STEP 4 Click **Save**.

The profile is added to the **Profile Table**.

To edit a PPPoE profile listed in the **Profile Table**, select the profile and click **Edit**. To delete selected profiles, click **Delete**.

Configuring the LAN (Local Network) Settings

If you have an IPv4 network, use these sections to configure your LAN settings. If you have an IPv6 network, see [Configuring IPv6 LAN Properties, page 43](#).

Configuring IPv4 LAN (Local Network) Settings

If you have an IPv4 LAN, you can configure the following settings:

Configuring the Host Name

To configure the host name of the Cisco RV120W:

-
- STEP 1** Choose **Networking > LAN (Local Network) > IPv4 LAN (Local Network)**.
 - STEP 2** In the **Host Name** field, enter the host name of the Cisco RV120W. You can use only alpha-numeric characters and the hyphen.

The default hostname (for example, “router9BA120”) consists of the word “router” followed by the last 3 bytes of firewall’s LAN MAC address (in Hex-decimal form). This format allows the FindIT application to use Bonjour to identify Cisco Small Business devices on the LAN.
 - STEP 3** Click **Save**.
-

Configuring the IP Address

You might want to change the default IP address if that address is assigned to another piece of equipment in your network.

To configure the IP address of the Cisco RV120W:

STEP 1 Choose **Networking > LAN (Local Network) > IPv4 LAN (Local Network)**.

STEP 2 Enter this information:

IP Address	Enter the LAN IP address of the RV120W. Make sure the address is not in use by another device on the same network. The default IP address is 192.168.1.1.
Subnet mask	Choose the subnet mask for the new IP address from the drop-down menu. The default subnet is 255.255.255.0.

STEP 3 Click **Save**.

After changing the Cisco RV120W's LAN IP address, your PC is no longer connected to the Cisco RV120W.

STEP 4 To reconnect your PC to the Cisco RV120W:

- If DHCP is configured on the Cisco RV120W, release and renew your PC's IP address.
- If DHCP is not configured on the Cisco RV120W, manually assign an IP address to your PC. The address must be on the same subnet as the Cisco RV120W. For example, if you change the Cisco RV120W's IP address to 10.0.0.1, assign your PC an IP address in the range of 10.0.0.2 to 10.0.0.254.

STEP 5 Open a new browser window and enter the new IP address of the Cisco RV120W to reconnect.

Configuring DHCP

By default, the Cisco RV120W 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 firewall'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.

For most applications, the default DHCP 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.

To configure the DHCP settings of the Cisco RV120W:

STEP 1 Choose **Networking > LAN (Local Network) > IPv4 LAN (Local Network)**.

STEP 2 From the **DHCP Mode** drop-down menu, choose one of these options:

- **None**—Choose this option if the Cisco RV120W is not going to act as a DHCP server.
- **DHCP Server**—Choose this option to configure the Cisco RV120W to be a DHCP server and enter this information:
 - **Domain Name**— (Optional) Enter the domain name for your network.
 - **Starting IP Address/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 Cisco RV120W's LAN IP address.
 - **Primary DNS Server/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 option to configure the Cisco RV120W to be a DHCP relay agent and enter the address of the relay agent in the **Relay Gateway** field. The relay agent transmits DHCP messages between multiple subnets.

STEP 3 Click **Save**.

Configuring the DNS Proxy

You can also enable a DNS proxy. When enabled, the firewall 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.

To configure the DNS proxy server for the Cisco RV120W:

-
- STEP 1** Choose **Networking > LAN (Local Network) > IPv4 LAN (Local Network)**.
 - STEP 2** In the **DNS Proxy** field, check to enable the Cisco RV120W to act as a proxy for all DNS requests and communicate with the ISP's DNS servers.
 - STEP 3** Click **Save**.
-

Configuring Virtual LAN (VLAN) Membership

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 (Local Network) > VLAN Membership**.
 - STEP 2** Check the **Enable** box.
 - STEP 3** Click **Save**.
-

Underneath the **Enable VLAN** field, The VLAN Membership Table is shown. This shows available VLANs, including the VLAN ID, description, ports, and whether inter-VLAN routing is enabled or not for each configured VLAN.

Creating a VLAN

You can create up to four VLANs on the Cisco RV120W.

-
- STEP 1** Choose **Networking > LAN (Local Network) > VLAN Membership**.
 - STEP 2** In the **VLAN Membership Table**, click **Add Row**.
 - STEP 3** 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 4** Enter a description for the VLAN.
- STEP 5** To enable routing between this and other VLANS, check the **Inter VLAN Routing** box.
- STEP 6** To enable device management, check the **Device Management** box. This allows you to access the Device Manager from that VLAN. For example, if you created a VLAN with the VLAN ID of 2 and enabled device management, you can access the Device Manager by using the first IP address on the created VLAN (for example, 192.168.2.1).
- STEP 7** Under each of the ports for the VLAN, choose one of the following:
- **Tagged**—Used when connecting to switches carrying multiple VLANs.
 - **Untagged**—Access ports connecting to end devices like printers and workstations.
- STEP 8** 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 RV120W 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 RV120W.

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 Static DHCP

You can configure a static 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 (Local Network) > 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 IPs should be outside this pool. The DHCP server will then serve the reserved IP address when the device using the corresponding MAC address requests an IP address.

- STEP 5** Click **Save**.

Configuring Advanced DHCP Settings

Configuring Automatic Configuration Download

You can configure the Cisco RV120W to download a configuration file from a TFTP server. Upon rebooting, the firewall downloads the file.

To configure automatic configuration download:

- STEP 1** Choose **Networking > LAN (Local Network) > Advanced DHCP Configuration**.
- STEP 2** Check **Enable** to enable downloading of configuration files.
- STEP 3** Choose the TFTP server type:
- **Host Name**—Enter the host name of the TFTP server in the TFTP server host name field.
 - **Address**—Enter the IP address of the TFTP server in the TFTP Server IP field.
- STEP 4** Click **Save**.

Adding a DHCP Client to Configuration File Map

This table displays the list of currently configured DHCP Client MAC address to configuration filename mappings. It has the following fields:

- MAC Address
- Configuration Filename

Click **Add** to add a new DHCP Client MAC address to configuration filename mapping. Click **Edit** to edit the MAC address or boot filename for a particular entry. Click **Delete** to delete a particular entry.

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 Routing

Choosing the Routing Mode

The Cisco RV120W provides two different routing modes. Network Address Translation (NAT), or gateway routing, 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 firewall is configured with a single “public” IP address. The Cisco RV120W 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 RV120W are assigned IP addresses from a private subnet (for example, 192.168.10.0).

The other routing mode, “router,” 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 Routes, page 37](#), or [Configuring Dynamic Routing, page 38](#).

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.

STEP 3 Click **Save**.



NOTE If you have already configured DMZ or firewall settings on your firewall in gateway (NAT) mode, selecting “router” changes those settings back to the default.

Viewing Routing Information

To view routing information your network:

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

STEP 2 Next to the type of network you have, click **Display**.

Information about your network routing is displayed, including the following:

IPv4 Routing Table

- 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:
 - UP—Route is up.
 - Host—Target is a host.

- Gateway—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).
- Interface—Interface to which packets for this route will be sent.
- Type—Type of routing used (RIP or static).

IPv6 Routing Table

- Destination—Destination host/network IP address for which this route is added.
- Next Hop—IP address of an adjacent or intermediate host or router through which traffic must flow before reaching its ultimate destination.
- Flags—For debugging purpose only; possible flags include:
 - UP—Route is up.
 - Host—Target is a host.
 - Gateway—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).
- **Interface**—Interface to which packets for this route will be sent.
- **Type**—Type of routing used (RIP or static).

Configuring Static Routes

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 Routes**.
 - STEP 2** In the **Static Route Table**, click **Add**.
 - STEP 3** In the **Route Name** field, enter the name of the route.
 - STEP 4** If a route is to be immediately active, check the **Active** check 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 firewall. 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** check 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 firewalls 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** From the **Interface** drop-down menu, 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 firewall is used to connect your network to the Internet, then your gateway IP is the firewall'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 Cisco RV120W 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 RV120W.

To configure dynamic routing:

- STEP 1** Choose **Networking > Routing > Dynamic Routing**.
- STEP 2** To configure how the firewall sends and receives RIP packets, choose the RIP direction:
- **None**—The firewall neither broadcasts its route table nor does it accept any RIP packets from other routers. This option disables RIP.
 - **In Only**—The firewall accepts RIP information from other router, but does not broadcast its routing table.

- **Out Only**—The firewall broadcasts its routing table periodically but does not accept RIP information from other routers.
- **Both**—The firewall both broadcasts its routing table and also processes RIP information received from other routers.

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 2**.)

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 RV120W 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** In the **Port Management Setting Table**, 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 Negotiation** box to let the firewall 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** Check the **Flow Control** box to enable flow control.
 - STEP 5** (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 6** (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 7** 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 firewall 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. In the **Update Period** field, enter the number of hours before the Cisco RV120W updates the host information on DynDNS.com.

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. In the **Update Period** field, enter the number of hours before the Cisco RV120W updates the host information on TZO.com.

STEP 4 Click **Save**.

Configuring IPv6

If you have an IPv6 network, see the following sections.

Configuring the IP Mode

To configure IPv6 properties on the Cisco RV120W, set the IP mode to IPv6:

-
- STEP 1** Choose **Networking > IPv6 > IP Mode**.
 - STEP 2** Click the **IPv4 and IPv6 Dual-Stack** radio button.
 - STEP 3** Click **Save**.
-

Configuring IPv6 WAN Settings

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

The Cisco RV120W 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 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** Choose **IPv6 > IPv6 WAN (Internet)**.
 - STEP 2** In the **WAN (Internet) Address (IPv6)** field, choose **DHCPv6**.
 - STEP 3** 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, an ICMPv6 discover message will originate from the Cisco RV120W and is used for auto-configuration.
 - STEP 4** Click **Save**.
-

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** Choose **IPv6 > IPv6 WAN (Internet)**.
 - STEP 2** In the **WAN (Internet) Address (IPv6)** field, choose **Static IPv6**.
 - STEP 3** Enter the IPv6 IP address assigned to your firewall.
 - STEP 4** 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 5** Enter the default IPv6 gateway address, or the IP address of the server at the ISP that this firewall will connect to for accessing the internet.
 - STEP 6** 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 7** 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 > IPv6 > IPv6 LAN (Local Area Network)**.
 - STEP 2** Under **LAN TCP/IP Setup**, in the **IPv6 Address** field, enter the IP address of the Cisco RV120W. 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 RV120W 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 RV120W. 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 firewall 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 RV120W'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 > IPv6 > IPv6 LAN (Local Area Network)**.
 - STEP 2** In the **IPv6 Address Pool Table**, click **Add**.
 - STEP 3** Enter the starting IP address and ending IP address of the pool.
 - STEP 4** Enter the prefix length. The number of common initial bits in the network's addresses is set by the prefix length field.
 - STEP 5** Click **Save**.
-

Configuring IPv6 Routing

To configure IPv6 routing, see the following sections.

Configuring Dynamic Routing

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 RV120W, RIPng is disabled by default.

To configure RIPng:

-
- STEP 1** Select **Networking > IPv6 > Routing**.
 - STEP 2** Under **RIPng**, check **Enable**.
 - STEP 3** Click **Save**.
-

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 > IPv6 > 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 firewall. 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**—The route goes through the WAN interface.
 - **LAN**—The route goes through the LAN interface.

- **6 to 4 Tunnel**—Uses the tunnel interface to route traffic from an IPv6 network to other IPv6 networks over an IPv4 network.

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 Tunneling

The Cisco RV120W provides several IPv6 tunneling methods. 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.



NOTE You must use static routes when tunneling. See [Configuring Static Routing, page 46](#).

To configure 6to4 Tunneling:

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

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

STEP 3 Click **Save**.

Viewing IPv6 Tunnel Information

To view IPv6 tunnel information, choose **Networking > IPv6 > Tunneling**. Click **Refresh** to get the latest information.

The IPv6 Tunnel Status table shows the name of tunnel and the IPv6 address that is created on the device.

Configuring Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) Tunnels

Intra-site automatic tunnel addressing protocol (ISATAP) is a method to transmit IPv6 packets between dual-stack nodes over an IPv4 network. The Cisco RV120W 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 > Tunneling**.
 - STEP 2** In the **ISATAP Tunnel Table**, click **Add**.
 - STEP 3** Enter the tunnel name.
 - STEP 4** Choose the local endpoint address, or the endpoint address for the tunnel that starts with the Cisco RV120W. The endpoint can be the LAN interface (if the LAN is configured as an IPv4 network), or another LAN IPv4 address.
 - STEP 5** If you chose **Other IP** in Step 4, enter the IPv4 address of the endpoint.
 - STEP 6** 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 7** Click **Save**.

To modify the settings of an ISATAP tunnel:

-
- STEP 1** Choose **Networking > IPv6 > Tunneling**.
 - STEP 2** Check the check boxes for the tunnels you want to modify.
 - STEP 3** Click **Edit**, make the changes, and click **Save**.
-

To delete an ISATAP tunnel:

-
- STEP 1** Choose **Networking > IPv6 > Tunneling**.
 - STEP 2** Check the check boxes for the tunnels you want to delete.
 - STEP 3** Click **Delete**.
-

Configuring Router Advertisement

The Router Advertisement Daemon (RADVD) on the Cisco RV120W listens for router solicitations in the IPv6 LAN and responds with router advertisements as required. This is stateless IPv6 auto configuration, and the Cisco RV120W distributes IPv6 prefixes to all nodes on the network.

To configure the RADVD:

-
- STEP 1** Choose **Networking > IPv6 > Router Advertisement**.
 - STEP 2** Under **Router Advertisement 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. ($\text{MinRtrAdvInterval} = 0.33 * \text{MaxRtrAdvInterval}$.) 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**.

Configuring Router Advertisement Prefixes

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/Local/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**.

Configuring the Wireless Network

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

- [A Note About Wireless Security, page 51](#)
- [Understanding the Cisco RV120W's Wireless Networks, page 54](#)
- [Configuring Basic Wireless Settings, page 54](#)
- [Configuring Advanced Wireless Settings, page 61](#)
- [Configuring Wi-Fi Protected Setup, page 62](#)
- [Configuring a Wireless Distribution System \(WDS\), page 63](#)

A Note About Wireless Security

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

- [Wireless Security Tips, page 52](#)
- [General Network Security Guidelines, page 53](#)

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 RV120W's Wireless Networks

The Cisco Small Business RV 120W Wireless-N VPN Firewall provides four separate virtual wireless networks. These networks can be configured and enabled with individual settings. You can set up the 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.

Configuring Basic Wireless Settings

The following sections contain information on how to configure basic wireless settings on the Cisco RV120W. These settings apply to all of the wireless networks.

Configuring Radio, Mode, and Channel Settings

-
- STEP 1** Choose **Wireless > Basic Settings**.
- STEP 2** In the **Radio** field, choose **Enable** to enable wireless functionality for the Cisco RV120W. Choosing **Disable** turns off wireless functionality for the firewall.
- STEP 3** In the **Wireless Network Mode** field, choose the type of wireless network based on the devices you have that will connect to the network:
- **B/G Mixed**—Select this mode if you have devices in the network that support 802.11b and 802.11g.
 - **G Only**—Select this mode if all devices in the wireless network only support 802.11g.
 - **B/G/N Mixed**—Select this mode if you have devices in the network that support 802.11b, 802.11g and 802.11n.
 - **N Only**—Select this mode only if all devices in the wireless network support 802.11n.
- STEP 4** Select the channel bandwidth. Available choices depend on the wireless network mode chosen in Step 3.
- STEP 5** The **Control Side Band** 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 6** The channel field specifies the frequency that the radio uses to transmit wireless frames. Select a channel from the list of channels or choose **auto** to let the Cisco RV120W determine the best channel to use based on the environment noise levels for the available channels.
- STEP 7** In the **U-APSD** field, choose **Enable** to enable the Unscheduled Automatic Power Save Delivery (also referred to as WMM Power Save) feature that allows the radio to conserve power. This feature is disabled by default.
- STEP 8** Click **Save**.

Configuring Wireless Security and Other Settings

At a minimum, you should edit the default profiles to enable wireless security. See [A Note About Wireless Security, page 51](#).

You can configure wireless security and other settings for each wireless network. To configure wireless settings:

-
- STEP 1** Choose **Wireless > Basic Settings**.
 - STEP 2** In the **Wireless Basic Settings Table**, check the box on the left of the wireless network you want to configure.
 - STEP 3** Click **Edit** to configure these network properties:
 - a. Enter the **SSID name**, or the 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.
 - b. 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).
 - c. Enter the **VLAN**, or network for this wireless network. (See Chapter 2, Configuring Networking, for more information on VLANs.) Devices connecting to this network are assigned addresses on this VLAN. The default VLAN is 1 and if all the devices are on the same network, this can be left unchanged.

- d. (Optional) Check the **Wireless Isolation within SSID** box to separate this network from the other three networks on the Cisco RV120W. When this feature is enabled, the network can communicate with the Cisco RV120W, but not with any of the other networks.
- e. In the **Max Associated Clients** field, enter the maximum number of endpoints that can connect to this network. 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. The number of clients connected across all four virtual access points cannot exceed 100.
- f. Click **Save**.

Configuring Security

- STEP 1** Choose **Wireless > Basic Settings**.
- STEP 2** In the **Wireless Basic Settings Table**, check the box on the left of the wireless network you want to configure.
- STEP 3** Click **Edit Security Mode** to configure security.
- STEP 4** Select the SSID to configure.
- STEP 5** Click **Enable** under **Wireless Isolation within SSID** to separate this network from the other three wireless networks on the Cisco RV120W. When this feature is enabled, the network can communicate with the Cisco RV120W, but not with any of the other three networks.
- STEP 6** In the **Security** field, select the type of security. All devices on this 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.

The **Encryption Type** appears based on the type of network you chose in Step 3:

- WPA Personal, WPA Enterprise, WPA2 Personal Mixed, WPA2 Enterprise Mixed—TKIP+AES
- WPA2 Personal, WPA2 Enterprise—AES

STEP 7 If you chose **WEP**:

- 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 WEP)**. The larger size keys provide stronger encryption, making the key more difficult to crack (for example, 64-bit WEP has a 40-bit key which is less secure than the 128-bit WEP, which has a 104-bit key).
- c. (Optional) In the **WEP Passphrase** field, enter an alphanumeric phrase (longer than eight characters for optimal security) and click **Generate Key** to generate four unique WEP keys in the WEP Key fields below.
- d. Select one of the four keys 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 7c, 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”.

If you chose **WPA Personal**, **WPA2 Personal**, or **WPA2 Personal Mixed**:

- a. Enter the **WPA Key**, or password/phrase that will secure the network. Devices connecting to the network must use this phrase for authentication.
- b. If you want to see the password as you are entering it, check the **Unmask Password** box.
- c. In the **Key Renewal** field, enter the number of seconds after which the Cisco RV120W will generate a new key. These keys are internal keys exchanged between the Cisco RV120W and connected devices. The default value (3600 seconds) is usually adequate unless you are experiencing network problems.

If you chose **WPA Enterprise** or **WPA2 Enterprise Mixed**, no further configuration is required.

If you chose **WPA2 Enterprise**, you can check the **Pre-Authentication** box (optional). Pre-authentication allows wireless clients to quickly switch between connected wireless networks sharing the same security configuration. When a wireless client disconnects from a wireless network, a notification is sent to the network, which then sends the pre-authentication info to other wireless networks.

STEP 8 Click **Save**.

Configuring 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 wireless network.

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

STEP 2 In the **Wireless Basic Settings Table**, check the box on the left of the wireless network you want to configure.

STEP 3 Click **Edit MAC Filtering**.

STEP 4 Choose **Enable**.

STEP 5 Under **Connection Control**, choose one of the following:

- **Block following MAC addresses from connecting to wireless network—** Blocks MAC addresses specified below from connecting to the wireless network.
- **Allow only following MAC addresses to connect to wireless network—** Allows only the MAC addresses specified below to connect to the wireless network.

STEP 6 Enter the MAC addresses of the endpoints to allow or deny. To see a list of currently-connected clients, click **Wireless Clients List**.

STEP 7 Click **Save**.

Configuring Wi-Fi Multimedia

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

To configure WMM:

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

STEP 2 In the **Wireless Basic Settings Table**, check the box on the left of the wireless network you want to configure.

STEP 3 Click **Edit WMM**.

STEP 4 In the SSID field, select SSID that clients use to connect to the AP.

STEP 5 Check the **WMM Enable** box to enable WMM based on the IEEE 802.11e standard for this profile. WMM helps in prioritizing wireless traffic according to four access categories:

- Voice (highest priority, 4)
- Video (high priority, 3)
- Best effort (medium priority, 2)
- Background (lowest priority, 1)

STEP 6 In the **DSCP to Queue** table, for each ingress DSCP, you can choose the output queue for the traffic. The Differentiated Services Code Point (DSCP) field identifies

the data packet and the output queue identifies the output queue in which the packet is transmitted:

- Voice (4) or Video (3)—High priority queue, minimum delay. Typically used to send time-sensitive data such as video and other streaming media.
- Best Effort (2)—Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue.
- Background (1)—Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is typically sent to this queue (FTP data, for example).

If you want to change the output queue for packets marked with a particular DSCP, select the new output queue from the drop-down list.

STEP 7 Click **Save**.

Configuring Wireless Network (SSID) Scheduling

You can configure each of the four available wireless networks on the Cisco RV120W to be active during certain times of the day. To configure the schedule for a wireless network:

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

STEP 2 In the **Wireless Basic Settings Table**, check the box on the left of the wireless network you want to configure.

STEP 3 Click **Edit SSID Scheduling**.

STEP 4 Select the wireless network for which you want to create a schedule.

STEP 5 Check the **Enable** box to allow you to create a schedule to make the network active during certain times.

STEP 6 Enter the start and stop times for the network to be active.

STEP 7 Click **Save**.

Configuring Advanced Wireless Settings

To configure advanced wireless settings on the Cisco RV120W:

- STEP 1** Choose **Wireless > Advanced 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 RV120W 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 μ s for transmission, or it may be an optional “short” preamble that requires only 96 μ s. 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 RV120W's ability to catch all wireless transmissions but severely decreases performance.

STEP 8 The **Short Retry Limit** and **Long Retry Limit** fields determine the number of times the Cisco RV120W 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 9 Click **Save**.

Configuring Wi-Fi Protected Setup

You can configure Wi-Fi Protected Setup (WPS) on the Cisco RV120W to allow WPS-enabled devices to more easily connect to the wireless network.

STEP 1 Choose **Wireless > WPS**.

STEP 2 In the **VAP** field, select the wireless network on which you want to enable WPS. The network must use WPA, WPA2, or WPA+WPA2 security.



NOTE You can enable WPS on only **one** of the four networks, or virtual access points.

STEP 3 Under **WPS Status**, choose **Enable** to allow WPS configuration. 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 Choose the WPS setup method:

- Setup Using a PIN—In the **WPS Setup Method** section, in the **Station PIN** field, enter the personal identification number (PIN) of the device you want to connect to the network. You must log in to that device to obtain its WPS PIN. Then click **Configure via PIN**. After clicking this button on the Cisco RV120W, on the WPS-enabled device, select the necessary option to begin WPS. The device should begin communication with the Cisco RV120W.
 - Setup Using a WPS Button—If the device you want to connect has a WPS button, push the button on the device. Then, on the Cisco RV120W, click **Configure via PBC** (push button configuration).
-

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** box to enable WDS in the Cisco RV120W.

STEP 3 Enter a **WPA Key** (password) for authentication.

STEP 4 Click **Save**.

You can manually add WDS peers that can connect to the Cisco RV120W:

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

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

Configuring the Firewall

This chapter contains information about configuring the firewall properties of the Cisco RV120W and includes the following sections:

- [Cisco RV120W Firewall Features, page 65](#)
- [Configuring Access Rules, page 67](#)
- [Configuring Attack Prevention, page 71](#)
- [Configuring Content Filtering, page 72](#)
- [Configuring URL Blocking, page 74](#)
- [Configuring Port Triggering, page 75](#)
- [Configuring Port Forwarding, page 76](#)
- [Configuring a DMZ Host, page 80](#)
- [Configuring Advanced Firewall Settings, page 80](#)
- [Firewall Configuration Examples, page 87](#)

Cisco RV120W Firewall Features

You can secure your network by creating and applying access rules that the Cisco RV120W uses to selectively block and allow inbound and outbound Internet traffic. You then specify how and to what devices the rules apply. You can configure 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.
- Rules for outbound (from your LAN to the Internet) or inbound (from the Internet to your LAN) traffic.

- 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.
- 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 network.

Inbound (Internet to LAN) 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 RV120W, 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 to Internet) 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 the 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 Access Rules

Configure access rules to control traffic to and from your network. To configure access rules, choose **Firewall > Access Rules**. All configured firewall rules on the Cisco RV120W are displayed in the Access Rule Table.

Configuring the Default Outbound Policy

You can configure the default outbound policy for the traffic that is directed from your secure network (LAN) to the Internet. The default *inbound* policy for traffic flowing from the Internet to your LAN is always blocked and cannot be changed. The *default outbound policy* applies to traffic that is not covered by the specific firewall rules that you have configured. For example, you may have specific firewall rules restricting outbound instant messaging and video traffic, but all other traffic would be permitted if you choose **allow** as the default outbound policy.

To configure the default outbound policy:

-
- STEP 1** Choose **Firewall > Access Rules**.
 - STEP 2** Under **Default Outbound Policy**, choose **Allow** or **Block**. **Allow** permits traffic from your LAN to the Internet. **Block** does not permit traffic from your LAN to the Internet.
 - STEP 3** Click **Save**.
-

Creating an Access Rule

Access rules specify the type of traffic that is allowed into and out of your network. To create access rules:

-
- STEP 1** Choose **Firewall > Access Rules**.
 - STEP 2** Click **Add Rule**.
 - STEP 3** Under Connection Type, choose the destination of traffic covered by this rule:
 - **Inbound**—Traffic from the Internet (WAN) to your network (LAN)
 - **Outbound**—Traffic from your network (LAN) to the Internet (WAN)

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. Choose the schedule from the drop-down list. See [Creating Firewall Schedules, page 84](#).
- **Allow by schedule, otherwise block**—Allows the selected type of traffic according to a schedule. Choose the schedule from the drop-down list. See [Creating Firewall Schedules, page 84](#).

STEP 5 Choose the service to allow or block for this rule. Choose **Any Traffic** 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)
- BOOTP_CLIENT (Bootstrap Protocol client)
- BOOTP_SERVER (Bootstrap Protocol server)
- CU-SEEME (videoconferencing) UDP or TCP
- DNS (Domain Name System), UDP or TCP
- FINGER
- FTP (File Transfer Protocol)
- HTTP (Hypertext Transfer Protocol)
- HTTPS (Secure Hypertext Transfer Protocol)
- ICMP (Internet Control Message Protocol) type 3 through 11 or 13
- ICQ (chat)
- IMAP (Internet Message Access Protocol) 2 or 3
- IRC (Internet Relay Chat)
- NEWS
- NFS (Network File System)
- NNTP (Network News Transfer Protocol)

- PING
- POP3 (Post Office Protocol)
- PPTP (Point-to-Point Tunneling Protocol)
- RCMD (command)
- REAL-AUDIO
- REXEC (Remote execution command)
- RLOGIN (Remote login)
- RTELNET (Remote telnet)
- RTSP (Real-Time Streaming Protocol) TCP or UDP
- SFTP (Secure Shell File Transfer Protocol)
- SMTP (Simple Mail Transfer Protocol)
- SNMP (Simple Network Management Protocol) TCP or UDP
- SNMP-TRAPS (TCP or UDP)
- SQL-NET (Structured Query Language)
- SSH (TCP or UDP)
- STRMWORKS
- TACACS (Terminal Access Controller Access-Control System)
- TELNET (command)
- TFTP (Trivial File Transfer Protocol)
- RIP (Routing Information Protocol)
- IKE
- SHTTPD (Simple HTTPD web server)
- IPSEC-UDP-ENCAP (UDP Encapsulation of IPsec packets)
- IDENT protocol
- VDOLIVE (live web video delivery)
- SSH (secure shell)
- SIP-TCP or SIP-UDP

STEP 6 In the **Source IP** field, configure the IP address to which the firewall rule applies:

- **Any**—The rule applies to traffic originating from any IP address in the local network.
- **Single Address**—The rule applies to traffic originating from a single IP address in the local network. Enter the address in the **Start** 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 **Start** field, and the ending IP address in the **Finish** field.

STEP 7 If you are configuring an **inbound** firewall access rule:

- a. Destination Network Address Translation (DNAT) maps a public IP address (your dedicated WAN address) to an IP address on your private network. In the **Send to Local Server (DNAT IP)** field, specify an IP address of a machine on the Local Network which is hosting the server.
- b. The router supports multi-NAT, so your Internet Destination IP address does not have to be the address of your WAN. 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. In this way, the LAN can be accessed from the internet by its aliased public IP address. Check the **Enable** box and enter the IP address you want to use.
- c. Under Rule Status, choose **Enabled** or **Disabled**. You may want to configure a rule and choose **Disabled** if you want to enable it at a later time.

If you are configuring an **outbound** firewall access rule:

- a. In the **Destination IP** field, configure the IP address to which the firewall rule applies:
 - **Any**—The rule applies to traffic going to any IP address.
 - **Single Address**—The rule applies to traffic going to a single IP address. Enter the address in the **Start** field.
 - **Address Range**—The rule applies to traffic going to an IP address located in a range of addresses. Enter the starting IP address in the **Start** field, and the ending IP address in the **Finish** field.
- b. You can configure Secure Network Address Translation (SNAT) to map a public IP address (your Dedicated WAN address, Optional WAN address, or another address) to an IP address on your private network. Under Use This SNAT IP Address, check **Enable** and enter the SNAT IP Address.

- c. Under Rule Status, choose **Enabled** or **Disabled**. You may want to configure a rule and choose **Disabled** if you want to enable it at a later time.

Configuring Attack Prevention

Attacks are malicious security breaches or unintentional network issues that render the Cisco RV120W unusable. Attack prevention allows you to manage WAN security threats such as continual ping requests and discovery via ARP scans. TCP and UDP flood attack prevention 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 suspend traffic from the offending source.

To configure attack prevention:

STEP 1 Choose **Firewall > Attack Prevention**.

STEP 2 Check the boxes to enable the following functions:

WAN (Internet) Security Checks

- **Respond to Ping on WAN (Internet)**—To configure the Cisco RV120W 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.
- **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.
- **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 (Local Network) Security Checks

- **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.

ICSA (International Computer Security Association) Settings

- **Block Anonymous ICMP Messages**—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 Content Filtering

The Cisco RV120W 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.

Enabling Content Filtering

To enable content filtering:

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

STEP 2 Check the **Enable** box.

STEP 3 Click **Save**.

Blocking Web Components

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.

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

STEP 2 With content filtering enabled, under Web Components, 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 3 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 [Enabling Content Filtering, page 72](#).

To add trusted domains:

- STEP 1** Choose **Firewall > Content Filtering**. The Trusted Domain Table displays a list of currently configured trusted domains.
- STEP 2** Click **Add** and enter the name of the trusted domain.
- STEP 3** Click **Save**.

Configuring URL Blocking

You can block access to websites that contain specific keywords in the URL or page contents. To configure URL blocking:

- STEP 1** Choose **Firewall > URL Blocking**. The table displays currently blocked keywords.
- STEP 2** Click **Add Row**.
- STEP 3** Under Status, check the box to enable blocking for the new keyword.
- STEP 4** Select the group to which to apply the keyword blocking. If you need to configure a new group, click Configure LAN Groups. (See [Configuring LAN \(Local Network\) Groups, page 86](#).)
- STEP 5** Enter the keyword to block.
- STEP 6** Click **Save**.

Configuring Port Triggering

Port triggering allows devices on the LAN to request one or more ports to be forwarded to them. Port triggering waits for an outbound request from the LAN 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, UDP, or both protocols.
- 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 Rule 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:

- **Action**—Whether to block or allow traffic (always or by schedule) that meets these filter rules, and when the rule is applicable.
- **Service**—Service for which this port forwarding rule is applicable.
- **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.
- **Source IP**—The source IP address for traffic from which traffic is forwarded (Any, Single Address or Address Range).
- **Destination IP**—The IP address of the server to which traffic is forwarded.
- **Forward From Port**—From which port traffic will be forwarded.
- **Forward To Port**—To which port traffic will be forwarded.

To configure port forwarding:

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

STEP 2 Click **Add**.

STEP 3 Choose the action:

- **Always Block**—Always block the selected type of traffic.
- **Always Allow**—Never block the selected type of traffic.
- **Block by Schedule**—Blocks the selected type of traffic according to a schedule. Choose the schedule from the drop-down list. See [Creating Firewall Schedules, page 84](#).
- **Allow by Schedule**—Allows the selected type of traffic according to a schedule. Choose the schedule from the drop-down list. See [Creating Firewall Schedules, page 84](#).

STEP 4 Under **Service**, select one of the common or custom services defined for this device:

- AIM (AOL Instant Messenger)
- BGP (Border Gateway Control)
- BOOTP_CLIENT (Bootstrap Protocol client)
- BOOTP_SERVER (Bootstrap Protocol server)
- CU-SEEME (videoconferencing) UDP or TCP
- DNS (Domain Name System), UDP or TCP
- FINGER
- FTP (File Transfer Protocol)
- HTTP (Hypertext Transfer Protocol)
- HTTPS (Secure Hypertext Transfer Protocol)
- ICMP (Internet Control Message Protocol) type 3 through 11 or 13
- ICQ (chat)
- IMAP (Internet Message Access Protocol) 2 or 3
- IRC (Internet Relay Chat)

- NEWS
- NFS (Network File System)
- NNTP (Network News Transfer Protocol)
- PING
- POP3 (Post Office Protocol)
- PPTP (Point-to-Point Tunneling Protocol)
- RCMD (command)
- REAL-AUDIO
- REXEC (Remote execution command)
- RLOGIN (Remote login)
- RTELNET (Remote telnet)
- RTSP (Real-Time Streaming Protocol) TCP or UDP
- SFTP (Secure Shell File Transfer Protocol)
- SMTP (Simple Mail Transfer Protocol)
- SNMP (Simple Network Management Protocol) TCP or UDP
- SNMP-TRAPS (TCP or UDP)
- SQL-NET (Structured Query Language)
- SSH (TCP or UDP)
- STRMWORKS
- TACACS (Terminal Access Controller Access-Control System)
- TELNET (command)
- TFTP (Trivial File Transfer Protocol)
- RIP (Routing Information Protocol)
- IKE
- SHTTPD (Simple HTTPD web server)
- IPSEC-UDP-ENCAP (UDP Encapsulation of IPsec packets)
- IDENT protocol

- VDOLIVE (live web video delivery)
- SSH (secure shell)
- SIP-TCP or SIP-UDP

STEP 5 Select the **Source IP**:

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

If you chose **Address Range** in Step 6, enter the starting IP address of the range in the **Start** field and the ending IP address of the range in the **Finish** field.

STEP 7 If you chose **Always Allow**, **Block by Schedule**, or **Allow by Schedule** in Step 3:

- a. Enter the Destination IP address, or the address where traffic meeting the rule should be sent.
- b. In the **Forward from Port** field, choose **Same as Incoming Port** if the traffic should be forwarded from the same port number on the outgoing server. Otherwise, choose **Specify Port** and enter the port number in the **Port Number** field.
- c. In the **Forward to Port** field, Choose **Same as Incoming Port** if the traffic should be sent to the same port on the receiving server. Otherwise, choose **Specify Port** and enter the port number in the **Port Number** field.

STEP 8 Click **Save**.

Configuring a DMZ Host

The Cisco RV120W 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 **Firewall > 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 [Creating Custom Services, page 83](#).
-

Configuring Advanced Firewall Settings

This page allows you to configure many advanced firewall settings.

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 > Advanced Settings > 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.
- **Range Length**—Range length maps one to one private address to public address up to the given range.
- **Service**—Shows configured services. Services for one-to-one NAT allow 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.

To add a one-to-one NAT rule:

STEP 1 Choose **Firewall > Advanced Settings > One-to-One NAT**.

STEP 2 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.
- **Range Length**—Range length maps one to one private address to public address up to the given range.
- **Service**—Choose the service for which the rule applies.

STEP 4 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 > Advanced Settings > 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 Allow the Rest**—Choose this option to block the traffic from the specified MAC addresses and to allow traffic from all other addresses.
- **Allow and Block the Rest**—Choose this option to allow 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 allow 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 “allow 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 In the MAC Addresses table, click **Add**.

STEP 4 Enter the MAC address and description to add to the table and click **Save**. Repeat for each address to allow or block.

STEP 5 Click **Save**.

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 RV120W sees packets with matching IP address but inconsistent MAC addresses, it drops those packets.

To configure IP/MAC Address binding:

-
- STEP 1** Choose **Firewall > Advanced Settings > 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** Click **Save**.
-

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 > Advanced Settings > Custom Services**.
 - STEP 2** Click **Add**.
 - STEP 3** Enter a service name for identification and management purposes.
 - STEP 4** Enter the service type, or layer 4 protocol that the service uses (**TCP, UDP, ICMP, ICMPv6, or other**).
- 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** If you chose TCP or UDP, in the **Start Port** field, enter the first TCP or UDP port of the range that the service uses. In the **Finish Port** field, enter the last TCP or UDP port of the range that the service uses.

If you chose **Other**, enter the number of the protocol in the Protocol Number field. (For example, if you are using RDP, enter 27 in the protocol number field.)

STEP 6 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 > Advanced Settings > Schedules**.

STEP 2 Click **Add**.

STEP 3 Enter a unique name to identify the schedule. This name is then available when you create access or port forwarding rules.

STEP 4 Under Time, check **All Day** if you want the schedule to apply to the entire day. Leave the box unchecked if you want it to only apply to certain hours of the day, and enter the specific start and end times, selecting **a.m.** or **p.m.**

STEP 5 Under Repeat, check **Everyday** to apply the schedule to all the days of the week. Leave the box unchecked if you want it to only apply to certain days, and check the boxes next to the days you want to include in the schedule.

STEP 6 Click **Save**.

Configuring Sessions

You can limit the maximum number of unidentified sessions and half-open sessions on the Cisco RV120W. 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 > Advanced Settings > 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 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 **Firewall > Advanced Settings > IGMP Configuration**.
 - STEP 2** Check the **Enable** box to allow IGMP communication between the router and other nodes in the network.
 - STEP 3** Choose the **Upstream Interface** (WAN or LAN). Select the interface (LAN or WAN) on which the IGMP proxy acts as a normal multicast client.
 - STEP 4** Click **Save**.
-

The Allowed Networks table lists all the allowed networks configured for the device and allows several operations on the allowed networks:

- **Network Address**—The network address from which the multicast packets originate.
- **Mask Length**— Mask Length for the network address.

In this table you can perform the following actions:

- **Check Box**—Select all the allowed networks in the table.
- **Delete**—Deletes the selected allowed network or allowed networks.
- **Add**—Opens the Allowed Network Configuration page to add a new network.
- **Edit**—Opens the Allowed Network Configuration page to edit the selected network.



NOTE

By default the device will forward multicast packets which are originating from its immediate WAN network.

Configuring LAN (Local Network) 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 [Configuring URL Blocking, page 74](#).)

To create a LAN Group:

-
- STEP 1** Choose **Firewall > Advanced Settings > LAN (Local Network) Groups**.
 - STEP 2** Click **Add**.
 - STEP 3** Enter the group name; spaces and quotes are not supported. Click **Save**.
 - STEP 4** Choose if the group consists of a single IP address, or an range of IP addresses.

If the group consists of a single IP address, enter the address in the **Start Address** field. If the group consists of a range of IP addresses, enter the address in the **Finish Address** field.
 - STEP 5** Click **Save**.
-

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 > Advanced 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 RV120W.
 - STEP 3** Click **Save**.
-

Firewall Configuration 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
Connection Type	Inbound
Action	Always Allow
Service	HTTP
Source IP	Any
Send to Local Server (DNAT IP)	192.168.5.2 (web server IP address)
Rule Status	Enabled

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
Connection Type	Inbound
Action	Always Allow
Service	CU-SEEME:UDP
Source IP	Address Range
Start	132.177.88.2
Finish	134.177.88.254
Send to Local Server (DNAT IP)	192.168.1.11
Rule Status	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
Connection Type	Inbound
Action	Always Allow
Service	HTTP
Source IP	Single Address
Start	10.1.0.52
Send to Local Server (DNAT IP)	192.168.1.2 (local IP address of your web server)
Rule Status	Enabled

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 > Advanced Settings > Schedules**.
- STEP 2** Click **Add**.
- STEP 3** Enter the schedule name (for example, "Weekend").
- STEP 4** Under Time, check **All Day**.
- STEP 5** Under **Repeat**, leave **Everyday** unchecked.
- STEP 6** Check **Saturday** and **Sunday**.
- STEP 7** Click **Save**.

Create an outbound access rule with the following parameters:

Parameter	Value
Connection Type	Outbound
Action	Block by Schedule
Schedule	Weekend
Service	HTTP
Source IP	Address Range
Start	starting IP address
Finish	ending IP address
Destination IP	Any
Rule Status	Enabled

Create an inbound access rule with the following parameters:

Parameter	Value
Connection Type	Inbound
Action	Block by Schedule
Schedule	Weekend
Service	All Traffic
Source IP	Any
Rule Status	Enabled

Configuring Virtual Private Networks (VPNs) and Security

This chapter describes VPN configuration, beginning with the **“Configuring VPNs”** section on page 92.

It also describes how to configure router security, beginning with the **“Configuring Security”** section on page 107.

The following sections are covered:

- **Configuring VPNs, page 92**
- **Configuring a Basic VPN, page 93**
- **Configuring Advanced VPN Parameters, page 94**
- **Configuring Security, page 107**

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, such as a PC running VPN client software, 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 119](#).
 - STEP 2** Create QuickVPN users. See [Configuring VPN Users, page 105](#). 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 7, 2000, XP, or Vista.”](#)

Configuring a Basic VPN

Use the basic VPN setup function to create a VPN with default values as proposed by the VPN Consortium (VPNC) and a Pre-shared Key (PSK). You can change these values later if you need to further configure any VPN parameters.

To configure a basic VPN:

-
- STEP 1** Choose **VPN > IPsec > Basic VPN Setup**.
 - STEP 2** Choose to which peers the VPN tunnel will connect:
 - **Gateway**—Connects the Cisco RV120W to a gateway using a secure tunnel.
 - **VPN Client**—Connects the Cisco RV120W to remote clients. The remote clients must run VPN client software.
 - STEP 3** Enter a name for the connection. The connection name is used for management.
 - STEP 4** Enter a pre-shared key. The VPN client or gateway will need to enter this key to establish the VPN connection.
 - STEP 5** Choose the type of address for the remote gateway, or the gateway to which the Cisco RV120W will connect:
 - **IP Address**—Enter the IP address of the gateway in the field below.
 - **FQDN (Fully-Qualified Domain Name)**—Enter the domain name in the field below (for example, <http://www.cisco.com>).

STEP 6 Choose the type of address for the local gateway (the Cisco RV120W):

- **IP Address**—Enter the IP address of the gateway in the box below.
- **FQDN** (Fully-Qualified Domain Name)—Enter the domain name in the box below (for example, <http://www.cisco.com>).

STEP 7 If you chose **gateway** in Step 2, enter the IP address and subnet mask of the remote LAN. The remote gateway to which the Cisco RV120W will connect is located on that LAN.



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**.

Viewing the Default VPN Settings

To view the default VPN settings:

STEP 1 Choose **VPN > IPsec > Basic VPN Setup**.

STEP 2 Click **View Default Settings**. Settings cannot be changed from this page, but can be configured through the **Basic VPN Setup** or **Advanced VPN Setup** menus.

Configuring Advanced VPN Parameters

The Advanced VPN Setup page allows you to configure advanced VPN parameters, such as IKE and other VPN policies. These policies control how the Cisco RV120W initiates and receives VPN connections with other endpoints.

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. Be sure to use compatible encryption, authentication, and key-group parameters for the VPN policy.

To configure IKE Policies:

-
- STEP 1** Choose **VPN > IPsec > Advanced VPN Setup**. In the IKE Policy table, click **Add**.
- STEP 2** Under **Policy Name**, enter a unique name for the policy for identification and management purposes.
- STEP 3** 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 4** Under **Exchange Mode**, choose one of the following options:
- **Main**—This mode negotiates the tunnel with higher security, but is slower.
 - **Aggressive**—This mode establishes a faster connection, but with lowered security.
-  **NOTE** If either the Local or Remote identifier type 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 5** In the **Local** section, under **Identifier Type**, choose the Internet Security Association and Key Management Protocol (ISAKMP) identifier for this router:
- **Local WAN (Internet) IP**
 - **FQDN**
 - **User-FQDN**
 - **DER ASN1 DN**

-
- STEP 6** If you chose **FQDN**, **User-FQDN**, or **DER ASN1 DN** as the identifier type, enter the IP address or domain name in the **Identifier** field.
- STEP 7** In the **Remote** section, under **Identifier Type**, choose the ISAKMP identifier for this router:
- **Remote WAN (Internet) IP**
 - **FQDN**
 - **User FQDN**
 - **DER ASN1 DN**
- STEP 8** If you chose **FQDN**, **User-FQDN**, or **DER ASN1 DN** as the identifier type, enter the IP address or domain name in the **Identifier** field.
-

IKE SA Parameters

The Security Association (SA) parameters define the strength and 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.
- Select **RSA-Signature** to disable the pre-shared key text field and use the Active Self Certificate uploaded in the Certificates page. A certificate must be configured in order for RSA-Signature to work.



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

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



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

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

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

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

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

Extended Authentication (XAUTH) Parameters

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

STEP 1 Select the XAUTH type:

- **None**—Disables XAUTH.
- **Edge Device**—Authentication is done by one of the following:
 - **User Database**—User accounts created in the router are used to authenticate users. See [Configuring VPN Users, page 105](#).
 - **RADIUS-PAP**—Authentication is done using a RADIUS server and password authentication protocol (PAP).
 - **RADIUS-CHAP**—Authentication is done using a RADIUS server and challenge handshake authentication protocol (CHAP).
- **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.

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 > Advanced VPN Setup**.

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

STEP 3 Enter a unique name to identify the policy.

STEP 4 Choose the **Policy Type**:

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

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. (See [Auto Policy Parameters, page 102.](#))

- STEP 5** 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 6** In the **NetBIOS** field, check the **Enable** 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.

Split DNS

Split DNS allows the Cisco RV120W to find the DNS server of the remote router without going through the ISP (Internet).

To enable split DNS:

STEP 1 Check the **Enable** box.

STEP 2 In the **Domain Name Server 1** field, specify a Domain Name server IP address, which is used only to resolve the domain configured in the **Domain Name 1** field.

STEP 3 In the **Domain Name Server 2** field, specify a Domain Name server IP address, which is used only to resolve the domain configured in the **Domain Name 2** field.

STEP 4 In the **Domain Name 1** field, specify a domain name, which will be queried only using the DNS server configured in the **Domain Name Server 1** field.

STEP 5 In the **Domain Name 2** field, specify a domain name, which will be queried only using the DNS server configured in the **Domain Name Server 2** field.



NOTE Make sure that you avoid using overlapping subnets for remote or local traffic selectors. Using these subnets would require adding static routes on the router and the hosts to be used.

For example, a combination to avoid would be:

Local Traffic Selector: 192.168.1.0/24

Remote Traffic Selector: 192.168.0.0/16

Manual Policy Parameters

If you chose **manual** as the policy type in Step 4, configure the 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

If you chose **auto** as the policy type in Step 4, configure the following:

-
- 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** Under **PFS Key Group**, check the **Enable** 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. (For information on creating these policies, see [Configuring IKE Policies, page 95](#).)

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 by performing one of the following actions:

- Choose **VPN > IPsec > Advanced VPN Setup** and click **IPsec VPN Connection Status**.
- Choose **Status > IPsec Connection Status**.

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 > Advanced VPN Setup** page.

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

Field	Description
Policy Name	IKE or VPN policy associated with this SA.
Endpoint	IP address of the remote VPN gateway or client.
Packets	Number of IP packets transmitted over this SA.
Kbytes	Kilobytes of data transmitted over this SA.
State	Status of the SA for IKE policies: Not Connected or IPsec SA Established.
Action	Choose Connect to establish a connection, or Drop to terminate an established connection.

Configuring VPN Users

To view a list of VPN users, choose **VPN > IPsec > VPN Users**. The VPN gateway authenticates users in this list when XAUTH is used in an IKE policy. QuickVPN clients can access only default LAN hosts.

Configuring a PPTP Server

If you are using a Point-to-Point Tunneling Protocol VPN server:

-
- STEP 1** Choose **VPN > IPsec > VPN Users**.
 - STEP 2** Under **PPTP Server**, check the **Enable** box.
 - STEP 3** Enter the IP address of the PPTP server.
 - STEP 4** In the **Starting IP Address** field, enter the starting IP address of the range of IPs to assign to connecting users.
 - STEP 5** In the **Ending IP Address field**, enter the ending IP address of the range of IPs to assign to connecting users.
-



NOTE The starting IP of the PPTP client IP range is used as the PPTP server IP of the Cisco RV120W and the remaining PPTP client IP address range is used to assign IP addresses to PPTP clients.

Adding New VPN Users

To add new users:

- STEP 1** Choose **VPN > IPsec > VPN Users**.
- STEP 2** In the **VPN Client Setting Table**, click **Add**.
- STEP 3** Check the **Enabled** box.
- STEP 4** Enter the username.
- STEP 5** Enter the password. If you want the user to be able to change the password, check the **Enabled** box.
- STEP 6** Under **Protocol**, choose the type of user:
 - **QuickVPN**—The user is authenticated by the VPN server. See [Creating Cisco QuickVPN Client Users, page 93](#).
 - **PPTP**—The user is authenticated by a PPTP server.
 - **XAUTH**—The user is authenticated by an external authorization server, such as a RADIUS server.
- 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 RV120W, 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 > IPsec > 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 RV120W provides several security methods, including certificate authentication, RADIUS server support, and 802.1x port-based authentication.

Using Certificates for Authentication

The Cisco RV120W 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.

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). 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 > SSL Certificate**. You can choose the following options:

Generating New Certificates

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** Choose **Security > SSL Certificate**.
 - STEP 2** Choose **Generate a New Certificate**.
 - STEP 3** Click **Generate Certificate**.
 - STEP 4** Enter the name of the certificate request.
 - STEP 5** 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 6** Choose the Hash Algorithm: MD5 or SHA-1. The algorithm used to sign the certificate (RSA) is shown.
 - STEP 7** Enter the signature key length, or the length of the signature (**512, 1024, or 2048**).
 - STEP 8** (Optional) Enter the IP address of the router.
 - STEP 9** (Optional) Enter the domain name of the router.
 - STEP 10** (Optional) Enter the e-mail address of the company contact that is used when generating the self certificate request.
 - STEP 11** Click **Generate**. A new certificate request is created.
-

Importing a Certificate from a File

To import a certificate from a file (for example, if you have been given a certificate from a CA), the file must be on a computer connected to the Cisco RV120W:

STEP 1 Choose **Security > SSL Certificate**.

STEP 2 Click **Import Certificate from a File**.

STEP 3 Click **Browse** to locate the certificate on the computer:

- **Trusted Certificate**—The certificate received from the Certificate Authority (for example, Microsoft, VeriSign, etc.)
- **Active Self Certificate**—The self certificate generated by the Cisco RV120W.

STEP 4 Click **Install Certificate**.

Exporting the Router's Current Certificate

To export the router's current certificate:

STEP 1 Choose **Security > SSL Certificate**.

STEP 2 Under **Export Certificate**, click the following:

- **Export for Admin**—Export the certificate for administrative backup purposes.
 - **Export for Client**—Export the certificate to be downloaded on an endpoint that will connect to the Cisco RV120W as a VPN client.
-

Using the Cisco RV120W 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:

- **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 RV120W re-authenticates with the RADIUS server.

- **Retries**—The number of retries for the Cisco RV120W 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 **RADIUS Server Table**, click **Add**.
 - STEP 2** In the **Authentication Server IP Address** field, enter the IP address of the authenticating RADIUS Server.
 - STEP 3** In the **Authentication Port** field, enter the port number on which the RADIUS server sends traffic.
 - STEP 4** In the **Secret** field, enter the shared key that allows the Cisco RV120W 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 RV120W re-authenticates with the RADIUS server.
 - STEP 6** In the **Retries** field, enter the number of retries for the Cisco RV120W 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 RV120W 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 RV120W 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**.

Configuring Quality of Service (QoS)

The Cisco RV120W lets you configure the following Quality of Service (QoS) features:

- [Configuring WAN QoS Profiles, page 112](#)
- [Configuring Profile Binding, page 114](#)
- [Configuring CoS Settings, page 115](#)
- [Mapping CoS Settings to DSCP Values, page 116](#)

Configuring WAN QoS Profiles

WAN QoS profiles let you manage the bandwidth of the traffic flowing from the secure network (LAN) to the insecure network (WAN).

You can configure WAN QoS profiles to control the rate at which the RV120W transmits data. For example, limiting the outbound traffic helps you prevent the LAN users from consuming all of the bandwidth of the Internet link.

Configuring Global Settings

To configure the WAN QoS global settings:

STEP 1 Choose **QoS > WAN QoS Profiles**.

STEP 2 Under **Global Settings**:

- To enable WAN QoS, check **Enable**.
- Set the WAN QoS mode by clicking the **Priority** or **Rate Limit** radio button.

The **Priority** option lets you allocate bandwidth based on a priority level.

The **Rate Limit** option lets you specify the total WAN bandwidth (**1–100 Mbps**).

For more information, see [Configuring Bandwidth Allocation Settings, page 113](#).

STEP 3 When prompted to reset the previous priority or rate limit configuration, click **OK**.

STEP 4 Click **Save**.

Configuring Bandwidth Allocation Settings

To configure the WAN QoS bandwidth allocation settings:

STEP 1 Choose **QoS > WAN QoS Profiles**.

STEP 2 Under **Priority Bandwidth Allocation Settings**:

If the WAN QoS mode is set to **Priority**, enter this information:

High Priority	Enter a value between 61 (default) and 100 .
Medium Priority	Enter a value between 31 (default) and 60 .
Low Priority	Enter a value between 10 (default) and 30 .

Each one of these values specifies the percentage of the total bandwidth (100 Mbps) allocated to these priority levels.

If the WAN QoS mode is set to **Rate Limit**, enter this information:

Total WAN (Internet) Bandwidth	Enter the total WAN bandwidth (1–100 Mbps).
---------------------------------------	---

STEP 3 Click **Save**.

Adding WAN QoS Profiles

To add a WAN QoS profile:

STEP 1 Choose **QoS > WAN QoS Profiles**.

STEP 2 In the **WAN QoS Profile Table**, click **Add**.

STEP 3 Enter this information:

Name	Enter the name of the profile.
Priority	If the WAN QoS mode is set to Priority , choose the priority level from the drop-down menu.
Minimum Bandwidth Rate	If the WAN QoS mode is set to Rate Limit , enter the minimum bandwidth rate (1 to total WAN bandwidth in Kbps).
Maximum Bandwidth Rate	If the WAN QoS mode is set to Rate Limit , enter the maximum bandwidth rate (100–1000000 Kbps).

STEP 4 Click **Save**.

STEP 5 To bind the profile to a traffic selector, see [Configuring Profile Binding, page 114](#).

Configuring Profile Binding

After creating WAN QoS profiles, you must bind them to traffic selectors.

To create a profile binding:

STEP 1 Choose **QoS > Profile Binding**.

STEP 2 In the **Available Profiles** field, choose a WAN QoS profile.

To create a profile, click **Configure Profile**. See [Configuring WAN QoS Profiles, page 112](#) for more information.

STEP 3 From the **Service** drop-down menu, choose the service the profile applies to.

If the service you are looking for is not in the drop-down menu, you can configure a custom service in the Firewall page (see [Creating Custom Services, page 83](#).)

STEP 4 From the **Traffic Selector Match Type** drop-down menu, choose the traffic selector to use to bind traffic to the profile.

STEP 5 Depending on the traffic selector you chose, enter this information:

Starting IP Address	Enter the starting IP address of the range.
Ending IP Address	Enter the ending IP address of the range.
MAC Address	Enter the MAC address for any client device (for example, a PC or wireless client) to which you want to assign the bandwidth.
VLAN ID	Choose the VLAN ID on the router to which the traffic selector applies.
DSCP Value	Enter the Differentiated Services Code Point (DSCP) value (0–63). This value determines how the traffic is prioritized.
Available SSIDs	Choose the SSID the selector applies to from the drop-down menu.

STEP 6 Click **Save**.

Configuring CoS Settings

You can map CoS priority settings to the traffic forwarding queue on the RV120W.

To map CoS priority settings to the traffic forwarding queue:

STEP 1 Choose **QoS > CoS Settings > Cos Settings**.

STEP 2 In the **CoS to Queue** field, check **Enable**.

STEP 3 For each CoS priority level in the **CoS to Traffic Forwarding Queue Mapping Table**, choose a priority value from the **Traffic Forwarding Queue** drop-down menu.

These values mark traffic types with higher or lower traffic priority depending on the type of traffic.

STEP 4 Click **Save**.

To restore the default CoS settings, click **Restore Default** and, when prompted, click **OK**. Then, click **Save**.

Mapping CoS Settings to DSCP Values



NOTE

Before you can map CoS settings to DSCP values, you must first enable the CoS to Queue option. See [Configuring CoS Settings, page 115](#) for more information.

To map CoS settings to DSCP values:

STEP 1 Choose **QoS > CoS Settings > CoS to DSCP**.

STEP 2 In the **CoS to DSCP** field, check **Enable**.

STEP 3 For each CoS priority level, enter the corresponding DSCP value (**0–63**).

The default value is **63**.

STEP 4 Click **Save**.

To restore the default CoS to DSCP mappings, click **Restore Default** and, when prompted, click **OK**. Then, click **Save**.

Administering Your Cisco RV120W

This chapter describes the administration features of the Cisco RV120W, including creating users, configuring network management, diagnostics and logging, date and time, and other settings. It contains the following sections:

- **Configuring Password Rules, page 118**
- **Using the Management Interface, page 118**
- **Configuring Network Management, page 121**
- **Configuring the WAN Traffic Meter, page 123**
- **Using Network Diagnostic Tools, page 125**
- **Capturing and Tracing Packets, page 126**
- **Configuring Logging, page 126**
- **Configuring the Discovery Settings, page 130**
- **Configuring Time Settings, page 132**
- **Backing Up and Restoring the System, page 132**
- **Upgrading Firmware, page 134**
- **Rebooting the Cisco RV120W, page 134**
- **Restoring the Factory Defaults, page 135**

Configuring Password Rules

The Cisco RV120W can enforce rules for passwords selected by administrators and users. To configure password rules:

-
- STEP 1** Choose **Administration > Password Rules**.
- STEP 2** Check the **Enable** box.
- STEP 3** In the **Individual Rule Settings** field, enter the rules you want the Cisco RV120W to enforce for passwords:
- **Minimal Password Length**—Enter the minimum password length.
 - **Minimal Number of Character Classes**—Enter the minimum number of character classes (for example, uppercase letters, lowercase letters, numbers, or special characters).
 - If you want the new password to be different than the old password, check **Enable**.
 - If you want to expire passwords, in the **Password Aging** field, check **Enable** and enter the **Password Aging Time**, or the number of days for the password to be active before it expires and the Cisco RV120W forces the user to choose a new password.



NOTE Passwords cannot be the same as the username, which is “admin” by default.

- STEP 4** Click **Save**.
-

Using the Management Interface

The Cisco RV120W provides a management interface to configure accounts for user and administrative access to the system.

Configuring Web Access

You can enable access on the LAN interface of the Cisco RV120W. If a user connects a PC to the LAN port, web access is then allowed using secure HTTP.

To enable web access on the LAN port:

-
- STEP 1** Choose **Administration > Management Interface > Web Access**.
- STEP 2** In the **LAN** section, under **HTTPS Web Access on LAN Interface**, check **Enable**.
-

Configuring Remote Management

You can enable remote access so that administrators can log in remotely to the system and access the web interface. To enable remote management:

-
- STEP 1** Choose **Administration > Management Interface > Remote Management**.
- STEP 2** Under **Remote Management**, check **Enable**.
- STEP 3** Choose the **Access Type**:
- **All IP Addresses**—The Cisco RV120W can be accessed from any IP address. Be sure to change the password if you select this option to prevent unauthorized persons from accessing your network.
 - **IP Address Range**—If you want to restrict access to certain computers, you can select a range of IP addresses. Only computers having IP addresses in this range can access the Cisco RV120W management interface. Choose one of the following:
 - **IP Address Range**—Allow access to the Cisco RV120W only from computers that have IP addresses in the specified range.
 - **Single IP Address**—Allow access to the Cisco RV120W only from a computer that has a specified IP address.
- STEP 4** If you chose **IP Address Range**, enter the start and end of the IP address number range. If you chose **Single IP Address**, enter the IP address.
- STEP 5** Enter the port number if you want to restrict access to only come from a specified port on the machine that is connecting remotely.
- STEP 6** You can enable Simple Network Management Protocol (SNMP), which allows you to 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 allow remote management of the Cisco RV120W by SNMP, under **Remote SNMP**, check **Enable**.

Configuring User Accounts

The Cisco RV120W 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 > Management Interface > User Accounts**.
 - STEP 2** Click either **Edit Admin Settings** or **Edit Guest Settings**.
 - 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 Session 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** In the **Administrator Inactivity Timeout** field, enter the number, in minutes, before an administrator login session times out due to inactivity.

-
- STEP 3** In the **Guest Inactivity Timeout** field, enter the number, in minutes, before a guest login session times out due to inactivity.
- STEP 4** Click **Save**.
-

Configuring Network Management

The Cisco RV120W supports Simple Network Management (SNMP) to allow you to 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.

Configuring SNMP

To configure SNMP:

-
- STEP 1** Choose **Administration > Network Management**.
- STEP 2** Under SNMP, check **Enable**.
- STEP 3** Click **Save**.
-

Editing SNMPv3 Users

SNMPv3 parameters can be configured for the two default Cisco RV120W user accounts (Admin and Guest). To configure:

-
- STEP 1** In the **SNMPv3 User 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 **Trap 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 Choose the SNMP Version: **v1**, **v2c**, or **v3**.

STEP 5 Enter the community string to which the agent belongs. Most agents are configured to listen for traps in the Public community.

STEP 6 Click **Save**.

Configuring Access Control Rules

The SNMP v1/v2c Access Control Table 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 **SNMP v1/v2c Access Control 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**.

STEP 2 You can enter the following information:

- **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**—The default system name is displayed. To change, click **Edit** and enter a name for easy identification of the router.

STEP 3 Click **Save**.

Configuring the WAN Traffic Meter

The WAN traffic meter displays statistics for traffic coming from the WAN (Internet) to the Cisco RV120W, and traffic going from the Cisco RV120W to the WAN.

To configure the WAN Traffic Meter:

STEP 1 Choose **Administration > WAN Traffic Meter**.

STEP 2 Under **WAN Traffic Meter**, to enable the display of WAN traffic statistics, check **Enable**.

STEP 3 Choose the type of traffic to display:

- **No Limit**—Display all traffic.
- **Download Only**—Only display traffic coming to the Cisco RV120W from the Internet.
- **Both Directions**—Display traffic coming to the Cisco RV120W from the Internet, and traffic going from the Cisco RV120W to the Internet.

STEP 4 If you want to limit traffic to or from the router, you can specify a size limit. When that size limit is reached, traffic is prevented from entering or exiting the router. Enter a number, in megabytes, in the **Monthly Limit** field.

STEP 5 To increase the monthly limit for that month, check **Increase this Month's Limit by:** and enter the additional megabytes for that month.

STEP 6 Click **Save**.

To restart the traffic counter:

STEP 1 Choose **Administration > WAN Traffic Meter**.

STEP 2 Under **Traffic Counter**, select **Restart Now**, or **Specific Time**, and enter the time you want the traffic counter to restart.

STEP 3 (Optional) Check the box to send an email report containing the traffic meter statistics before the counter is reset.

STEP 4 Click **Save**.

To configure what the Cisco RV120W does when the traffic limit is reached:

STEP 1 Choose **Administration > WAN Traffic Meter**.

STEP 2 Under **When Limit Is Reached**, select one of the following:

- **Block All Traffic**—All traffic to and from the Cisco RV120W is blocked.
- **Block All Traffic Except E-Mail**—Only email is allowed to and from the Cisco RV120W.

STEP 3 (Optional) Check the box to send an email alert when the traffic limit has been reached and traffic is being blocked.

STEP 4 Click **Save**.

To viewing traffic statistics, choose **Administration > WAN Traffic Meter**. Under **WAN (Internet) Traffic Statistics**, information is displayed about WAN traffic to and from the Cisco RV120W.

Using Network Diagnostic Tools

Using PING

PING can be used to test connectivity between this router and another device on the network connected to this router. To use PING:

STEP 1 Choose **Diagnostics > Network Tools**.

STEP 2 Under **Ping or Trace an IP Address**, enter an IP address or domain name and click **Ping**. A popup window appears, indicating the ICMP echo request status.

STEP 3 (Optional) Check the box if you want to allow PING traffic to pass through VPN tunnels.

Using Traceroute

Traceroute displays 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. To use traceroute:

STEP 1 Choose **Diagnostics > Network Tools**.

STEP 2 Under **Ping or Trace an IP Address**, enter an IP address or domain name and click **Traceroute**. A popup window appears with the hop information.

Performing a DNS Lookup

A DNS lookup can be performed to retrieve the IP address of a Web, FTP, Mail or any other Server on the Internet. To perform a DNS lookup:

-
- STEP 1** Choose **Diagnostics > Network Tools**.
 - STEP 2** Enter the **WAN (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

You can capture all packets that pass through a selected interface (LAN or WAN). To capture packets:

-
- STEP 1** Choose **Diagnostics > Capture Packets**.
 - STEP 2** Click **Packet Trace**; a new window appears.
 - STEP 3** Select the interface whose packets you want to trace 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



NOTE Enabling logging options may generate a significant volume of log messages and is recommended for debugging purposes only.

Configuring Logging Policies

To configure general logging policies:

-
- STEP 1** Choose **Administration > Logging > Logging Policies**.
 - STEP 2** The **Logging Policy Table** shows the types of logging that are configured on the system. To add a new type of logging, click **Add**.
 - STEP 3** Enter a name for the policy.
 - STEP 4** (Optional) Check **Enable** to log IPsec VPN events.
 - STEP 5** In the table, select the type of logs to capture for each severity. For example, you might want to log all types of events that have a severity level of “Emergency,” so you would check System, Kernel, and Wireless under “Emergency.”
 - STEP 6** Click **Save**.
-

Configuring Firewall Logs

To configure firewall logs:

-
- STEP 1** Choose **Administration > Logging > Firewall Logs**.
 - STEP 2** Under the type of routing logs, check the box to choose one or both of the following for each type:
 - **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” (see [Configuring the Default Outbound Policy, page 67](#)). For example, if **Accept Packets** is checked for **LAN to WAN** 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” (see [Configuring the Default Outbound Policy, page 67](#)). For example, if **Dropped Packets** is checked for **LAN to WAN** 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.)

STEP 3 Under the type of 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.

STEP 4 Under “other events 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.

STEP 5 Click **Save**.

Configuring Remote Logging

To configure remote logging:

STEP 1 Choose **Administration > Logging > Remote Logging Configuration**.

STEP 2 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.

STEP 3 Click **Save**.

Configuring Email Logging

STEP 1 Choose **Administration > Logging > Remote Logging Configuration**.

STEP 2 Select the check box to enable e-mail logs. Then enter the following:

- **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 box to configure the router to respond to an IDENT request from the SMTP server.

STEP 3 To confirm that the e-mail logs function is configured correctly, press **Test**.

STEP 4 (Optional) 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.

-
- STEP 5** Under **Logging Policy**, choose the type of logging policy. (See [Configuring Logging Policies, page 127](#).) By default, only IPsec VPN logs are enabled. Others are disabled.
- STEP 6** If you want the router to send logs to a Syslog server, check the box next to a syslog server field and enter the IP address or Internet Name of the Syslog server in the **Syslog Server** field. Choose the logging policy for each syslog server. You can configure up to 8 syslog servers.
- STEP 7** Click **Save**.
-

Configuring the Discovery Settings

The Cisco RV120W supports two types of discovery protocols: Bonjour and UPnP. Bonjour is a service advertisement and discovery protocol. Universal Plug and Play (UPnP) is a networking protocol that allows devices to discover each other and communicate on the network.

Configuring Bonjour

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.
- STEP 3** In the **Bonjour Interface Control Table**, you can see on which VLANs Bonjour is enabled. For example, Bonjour is by default enabled on the default VLAN ID 1. That means that the Cisco RV120W advertises itself to all devices connected to it on VLAN 1, and devices joining the network can connect to the Cisco RV120W. If you have other VLANs created on your network, you can enable Bonjour on those VLANs too. (See [Configuring Virtual LAN \(VLAN\) Membership, page 30](#) for more information.)
- STEP 4** Click **Save**.
-

Configuring UPnP

-
- STEP 1** Choose **Administration > Discovery Settings > Discovery - UPnP**.
- STEP 2** Check **Enable** to enable UPnP.
- STEP 3** In the **Advertisement Period** field, enter the number of seconds to specify how often this router will broadcast its UPnP information to all devices within range.
- STEP 4** In the **Advertisement Time to Live** field, enter the number of seconds for the advertisement to be active.

In the **UPnP Interface Control Table**, you can see on which VLANs UPnP is enabled. For example, UPnP is by default enabled on the default VLAN ID 1. That means that the Cisco RV120W advertises itself to plug and play devices connected to it on VLAN 1, and plug and play devices joining the network can connect to the Cisco RV120W. If you have other VLANs created on your network, you can enable UPnP on those VLANs too. (See [Configuring Virtual LAN \(VLAN\) Membership](#), page 30 for more information.)

The **UPnP Portmap Table** shows IP addresses and other settings of UPnP devices that have accessed the Cisco RV120W:

- **Active**—Indicates whether or not the port of the UPnP device that established a connection is currently active by displaying Yes or No.
 - **Protocol**—The network protocol (i.e. TCP, UDP, etc) that the device is using to connect to the Cisco RV120W.
 - **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 this router.
- STEP 5** Click **Save**.
-

Configuring 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. In the “From” and “To” fields, enter the month and day for which Daylight Saving Time will be active. In the **Daylight Saving Offset** field, choose the amount of time, in minutes, that the clock will be offset during daylight saving time.
 - STEP 4** Select whether to use a Network Time Protocol (NTP) server, or set the time and date manually.
 - STEP 5** If you chose NTP, choose to use either a default NTP server, or a custom NTP server.
 - STEP 6** If you chose to use a default NTP server, choose the server you want to use from the list. If you chose to use a custom NTP server, enter the server addresses or fully-qualified domain name.
 - STEP 7** If you chose to set the date and time manually, enter the date and time.
 - STEP 8** 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, select **Administration > Backup/Restore Settings**.

- 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.
- To save a copy of your router's startup configuration, click **Backup Startup Configuration**. The browser downloads the configuration file and prompts you to save the file on the PC.
- To save a copy of your router's mirror configuration, click **Backup Mirror Configuration**. The browser downloads the configuration file and prompts you to save the file on the PC.

The mirror image is the last working configuration. The startup configuration is the configuration that the device used to boot up. The startup and mirror configurations can differ. For example, if you made changes to the current configuration but forgot to save it, after 24 hours, the device automatically saves the currently-running configuration as the "mirror" image. But if the device crashed during the 24 hour window, then the device will use the startup configuration to boot up.

- To copy the mirror configuration file to the startup configuration file, click **Copy Mirror to Startup**. This replaces the startup configuration file with the mirror configuration file. You may want to do this if the device crashed and you had to reset the device to factory defaults. After you perform the factory reset, the mirror image is not erased, and you can copy it to the startup configuration to allow the device to use the configuration to boot up.
-

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 firmware version from the **Administration > Firmware Upgrade** page. To upgrade:

- STEP 1** Click **Browse**, locate and select the downloaded firmware, and click **Upload**.
 - STEP 2** (Optional) Check the box to reset all configuration and settings to the default values. **Do not check this box if you want to keep any settings you have changed on the router!**
 - STEP 3** Click **Start Firmware Upgrade**. 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 RV120W

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.

STEP 4 To restore factory defaults to the router, choose **Administration > Restore Factory Defaults**. Click **Default**.



CAUTION Do not perform this procedure unless you want to erase all configuration you have performed on the router.

Viewing the Cisco RV120W Status

This chapter describes how to view real-time statistics and other information about the Cisco RV120W.

- [Viewing the Dashboard, page 136](#)
- [Viewing the System Summary, page 139](#)
- [Viewing the Wireless Statistics, page 142](#)
- [IPsec Connection Status, page 143](#)
- [Viewing VPN Client Connection Status, page 144](#)
- [Viewing Logs, page 145](#)
- [Viewing Available LAN Hosts, page 146](#)
- [Viewing Port Triggering Status, page 147](#)
- [Viewing Port Statistics, page 148](#)
- [Viewing Open Ports, page 149](#)

Viewing the Dashboard

The **Dashboard** page provides you with a view of important router information.

To view the Dashboard:

STEP 1 Choose **Status > Dashboard**.

STEP 2 To display an interactive view of the router's back panel, click **Show Panel View**.

The view of the back panel shows you which ports are used (colored in green) and allows you to click the port to obtain information about the connection.

- To view a port's connection information, click the port.
- To refresh the port information, click **Refresh**.
- To close the port information sheet, click **Close**.

The **Dashboard** page displays the following:

Device Information

Host Name	The name of the device. To change the name, click Edit . See Configuring IPv4 LAN (Local Network) Settings, page 27 .
Firmware Version	The current software version the device is running.
Serial Number	The serial number of the device.

Resource Utilization

CPU	CPU utilization.
Memory	Memory utilization.
Current Time	Time of day.
System Up Time	How long the system has been running.

Syslog Summary

Indicates whether logging is enabled for these event categories:

- **Emergency**
- **Alert**
- **Critical**
- **Error**
- **Warning**

To view the logs, click **details**. For more information see [Viewing Logs, page 145](#).

To manage logs, click **manage logging**. For more information see [Configuring Logging, page 126](#).

LAN (Local Network) Interface

MAC Address	The MAC address of the router.
IPv4 Address	The local IP address of the router. To change the IP address, see Configuring the IPv4 WAN (Internet), page 20 .
DHCP Server	The status of the router's DHCP server (enabled or disabled). To configure the DHCP settings, see Configuring the IPv4 WAN (Internet), page 20 .

To view the LAN settings, click **details**. For more information see [Viewing Port Statistics, page 148](#).

WAN (Internet) Information

IP Address	The IP address of the router's WAN port. To change the IP address, see Configuring the WAN (Internet) Settings, page 19 .
State	The state of the Internet connection (up or down).

To view the WAN settings, click **details**. For more information see [Viewing Port Statistics, page 148](#).

Wireless Networks

Lists the status of the four wireless network SSIDs

To view the router's wireless settings, click **details**. For more information see [Viewing the Wireless Statistics, page 142](#).

VPN

Site-to-Site Tunnels	Displays the connected IPsec VPN tunnels.
PPTP Users	The number of Point-to-Point Tunneling Protocol (PPTP) users.
QuickVPN Users	The number of QuickVPN users.

Viewing the System Summary

The **System Summary** page displays a summary of the router's settings.

To view a summary of system settings:

-
- STEP 1** Choose **Status > System Summary**.
 - STEP 2** Click **Refresh** to obtain the latest information.
 - STEP 3** If applicable, to change a system setting, click its corresponding **Edit** link.
-

The **System Summary** page displays this information:

System Information

Host Name	The 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 version ID of the device.
Serial Number	The serial number of the device.

LAN (Local Network) Information

MAC Address	The MAC address of the device.
IPv4 Address	The IP address and subnet mask of the device.
IPv6 Address	The IP address and subnet mask of the device (shown only if IPv6 is enabled).
DHCP Server	The status of the router's DHCP server (enabled or disabled). If it is enabled, DHCP client machines connected to the LAN port receive their IP address dynamically.
DHCP Relay	Whether the device is acting as a DHCP relay.
DHCPv6 Server	Whether the device's DHCPv6 server is enabled or disabled. If it is enabled, DHCPv6 client systems connected to the LAN port receive their IP address dynamically.

WAN (Internet) Information (IPv4)

MAC Address	The MAC address of the WAN port.
Connection Time	The time duration for which the connection is up.
Connection Type	Shows weather 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	Shows weather the WAN port is connected to the Internet service provider.
DHCP Server	The IP address of the DHCP server to which the WAN port is connected.
Lease Obtained	The the time at which lease is obtained from the DHCP server.
Lease Duration	The duration for which the lease remains active.
IP Address	The WAN Address of the device.
Subnet Mask	The subnet mask of the WAN port.
Gateway	The gateway IP address of the WAN port.
Primary DNS Server	The IP address of the primary DNS server.
Secondary DNS Server	The IP address of the secondary DNS server.
NAT (IPv4 Only Mode)	

WAN (Internet) Information (IPv6)

Connection Time	The time duration for which the connection is up.
Connection Type	Shows weather the WAN IPv6 address is obtained dynamically through a DHCP server, assigned statically by the user, or obtained through a PPPoE/ PPTP/L2TP ISP connection.
Connection State	Shows weather the WAN port is connected to the ISP.
IP Address	The IP address of the WAN port.
Gateway	The gateway IP address of the WAN port.
DNS Server	DNS server IP address of the WAN port.

Wireless Information

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.

Channel

SSID	The name of the SSID.
MAC Address	The MAC address of the SSID.
Security	The security setting for the SSID.
Encryption	The encryption type used by the SSID.
Authentication	The authentication type used by the SSID.

Viewing the Wireless Statistics

The **Wireless Statistics** page shows a cumulative total of relevant wireless statistics for the radio on the device.

To view wireless statistics:

- STEP 1** Choose **Status > Wireless Statistics**.
- STEP 2** Click **Stop**.
- STEP 3** In the **Poll Interval** field, enter the number of seconds the router waits before updating the information on this page.
- STEP 4** Click **Start** to restart automatic refresh at the specified poll interval.

The **Wireless Statistics** page displays this information:

SSID	The name of the wireless network.
Packets	The number of received/sent wireless packets reported to the radio over all configured and active SSIDs.
Bytes	The number of received/sent bytes of information reported to the radio, over all configured APs.
Errors	The number of received/sent packet errors reported to the radio, over all configured APs.
Dropped	The number of received/sent 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.

NOTE The counters are reset when the device is restarted.

IPsec Connection Status

The **IPsec Connection Status** page displays the status of IPsec connections.

To view the status of IPsec connections:

-
- STEP 1** Choose **Status > IPsec Connection Status**.
 - STEP 2** Click **Stop**.
 - STEP 3** In the **Poll Interval** field, enter the number of seconds the router waits before updating the information on this page.
 - STEP 4** Click **Start** to restart automatic refresh at the specified poll interval.
-

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.
Kbytes	The data transmitted (in KB) over this SA.
Packets	The number of IP packets transmitted over this SA.
State	The current status of the SA for IKE policies. The status can be IPsec SA Established or IPsec SA Not Established.
Action	Click Connect to establish an inactive SA connection. Click Drop to terminate an active SA connection.

Viewing VPN Client Connection Status

The **VPN Client Connection Status** page displays the status of VPN connections.

To view VPN user connection status:

- STEP 1** Choose **Status > VPN Client Connection Status**.
- STEP 2** Click **Stop**.
- STEP 3** In the **Poll Interval** field, enter the number of seconds the router waits before updating the information on this page.
- STEP 4** Click **Start** to restart automatic refresh at the specified poll interval.

The **VPN Client Connection Status** page displays this information:

Username	The username of the VPN user associated with the QuickVPN or PPTP tunnel.
Remote IP	Displays the IP address of the remote QuickVPN client. This could be a 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 VPN user. ONLINE means that QuickVPN Tunnel, initiated/established by the VPN user, is active.
Start Time	The time of the VPN user establishing a connection.
End Time	The time of the VPN user ending a connection.
Duration	The duration between the VPN user establishing and ending a connection.
Protocol	The protocol the user uses, QuickVPN or PPTP.
Disconnect	Click to disconnect this user.

Viewing Logs

The **View Logs** page allows you to view the Cisco RV120W logs.

To view the logs:

-
- STEP 1** Choose **Status > View Logs**.
 - STEP 2** Click **Refresh Logs** to display the latest log entries.
 - STEP 3** To specify the types of logs to display, choose an option from the **Logging Policy** drop-down menu.
-

To delete all entries in the log window, click **Clear Logs**.

To email all log messages from the router, click **Send Logs**.

Viewing Available LAN Hosts

The **Available LAN (Local Network) Hosts** page displays information about the devices connected to the Cisco RV120W.

To view a list of all available LAN hosts:

STEP 1 Choose **Status > Available Local Network Hosts**.

STEP 2 From the **Filter** drop-down menu, choose the interface type.

You can choose one of the following options:

All	Displays a list of all devices connected to the router.
Wireless	Displays a list of all devices connected through the wireless interface.
Wired	Displays a list of all devices connected through the Ethernet ports on the router.

STEP 3 Click **Refresh** to display the latest LAN host information.

The **Available LAN (Local Network) Hosts** page displays the following fields:

Name	The name of the connected host.
IP Address	The IP address of the host.
MAC Address	The MAC address of the host.
Type	The type of connection (for example, static or dynamic).
Interface Type	The interface type (Wired or Wireless).

Viewing Port Triggering Status

To view the status of port triggering:

- STEP 1** Choose **Status > Port Triggering Status**.
- STEP 2** Click **Refresh** to display the latest port triggering information.

The **Port Triggering Status** window provides information on the ports that have been opened per the port triggering configuration rules. The ports are opened dynamically whenever traffic that matches the port triggering rules flows through them.

The **Port Triggering Status** page displays the following fields:

LAN (Local Network) 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

The **Port Statistics** page displays port statistics.

To view port statistics:

- STEP 1** Choose **Status > Port Statistics**.
- STEP 2** In the **Poll Interval** field, enter the auto-refresh time interval in seconds.
The default value is 10.
- STEP 3** To start the display of port statistics, click **Start**.

This page displays the latest port statistics based on the value you enter in the **Poll Interval** field. For example, if you enter a poll interval value of 5, the router refreshes the information on this page every 5 seconds.

This table displays the data transfer statistics for the Dedicated WAN, LAN, and WLAN ports, including the duration for which they were enabled.

The **Port Statistics** page displays this information:

Port	The name of the port.
Status	The status of the port (enabled or disabled).
Operational Mode	The bandwidth the port is operating at.
Packets	The number of received/sent packets per second.
Bytes	The number of received/sent bytes of information per second.
Frames	The number of received/sent frames per second.

Viewing Open Ports

The **View Open Ports** page displays a listing of all open ports.

To view open ports, choose **Status > View Open Ports**.

This page displays this information about open ports:

Proto	The protocol (TCP, UDP, and raw) used by the port.
Recv-Q	The number of bytes not copied by the program connected to this port.
Send-Q	The number of bytes not acknowledged by the program connected to this port.
Local Address	The address and port number of the local end of this socket.
Foreign Address	The address and port number of the remote end of this socket.
State	The state of the port.
PID/Program name	The process ID (PID) and name of the program using the port (for example, 1654/thttpd, where 1654 is the PID and thttpd is the program's name).

Using Cisco QuickVPN for Windows 7, 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 7, 2000, XP, or Vista. (Computers using other operating systems will have to use third-party VPN software.)

This appendix includes the following sections:

- [Before You Begin, page 150](#)
- [Installing the Cisco QuickVPN Software, page 151](#)
- [Using the Cisco QuickVPN Software, page 152](#)

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 119](#).
- STEP 2** Create Quick VPN user accounts. See [Configuring VPN Users, page 105](#). 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 RV120W CD-ROM into your CD-ROM drive. After the Setup Wizard begins, click the **Install QuickVPN** link.

The License Agreement window appears.

STEP 2 Click **Yes** to accept the agreement.

The InstallShield Wizard copies the appropriate files to the computer.

STEP 3 Click **Browse** and choose where to copy the files to (for example, C:\Cisco Small Business\QuickVPN Client).

STEP 4 Click **Next**.

STEP 5 Click **Finish** to complete the installation.

Downloading and Installing from the Internet

STEP 1 Open a web browser and enter the following URL:

<http://tools.cisco.com/support/downloads>

STEP 2 Enter RV120W 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.

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 VPN Users, page 105](#). In the **Server Address** field, enter the IP address or domain name of the Cisco RV120W. 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**.

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

-
- STEP 5** To terminate the VPN tunnel, click **Disconnect**. To change your password, click **Change Password**. For information, click **Help**.
- STEP 6** 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**.



NOTE You can change your password only if the **Allow User to Change Password** box has been checked for that username. See [Configuring VPN Users, page 105](#).

Where to Go From Here

Cisco provides a wide range of resources to help you obtain the full benefits of the Cisco RV120W.

Product Resources

Support	
Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport
Cisco Small Business Support and Resources	www.cisco.com/go/smallbizhelp
Phone Support Contacts	www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html
Cisco Small Business Firmware Downloads	www.cisco.com/go/software Select a link to download firmware for Cisco Small Business Products. No login is required.
Cisco Small Business Open Source Requests	www.cisco.com/go/smallbiz_opensource_request
Product Documentation	
Cisco RV120W	www.cisco.com/go/smallbizrouters
Cisco Small Business	
Cisco Partner Central for Small Business (Partner Login Required)	www.cisco.com/web/partners/sell/smb
Cisco Small Business Home	www.cisco.com/smb