



## ADMINISTRATION GUIDE

Cisco RV110W Wireless-N VPN Firewall

Revised in Sep.2014

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://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. (1110R)

---

<b>Chapter 1: Introduction</b>	<b>8</b>
Product Overview	8
Getting to Know the Cisco RV110W	10
Front Panel	10
Back Panel	12
Installing the Cisco RV110W	13
Placement Tips	13
Connecting the Equipment	13
Using the Setup Wizard	15
Using the Getting Started Page	16
Navigating through the Pages	18
Saving Changes	19
Viewing the Help Files	19
Configuration Next Steps	19
Verifying the Hardware Installation	19
Connecting to Your Wireless Network	20
<b>Chapter 2: Configuring Networking</b>	<b>22</b>
Configuring the WAN Settings	22
Configuring the LAN Settings	28
Changing the Default Cisco RV110W IP Address	29
Configuring DHCP	30
Configuring VLANs	31
Configuring Static DHCP	33
Viewing DHCP Leased Clients	34
Configuring a DMZ Host	34
Configuring RSTP	35
Port Management	36
Cloning the MAC Address	38
Configuring Routing	39
Viewing the Routing Table	41

Configuring Dynamic DNS	42
Configuring the IP Mode	43
Configuring IPv6	44
Configuring the WAN for an IPv6 Network	44
Configuring IPv6 LAN Settings	48
Configuring IPv6 Static Routing	51
Configuring Routing (RIPng)	53
Configuring Tunneling	53
Viewing IPv6 Tunnel Status	54
Configuring Router Advertisement	55
Configuring Advertisement Prefixes	56

### **Chapter 3: Configuring the Wireless Network** **61**

Wireless Security	61
Cisco RV110W Wireless Networks	63
Configuring Basic Wireless Settings	64
Editing the Wireless Network Settings	65
Configuring the Security Mode	66
Configuring MAC Filtering	70
Configuring Time of Day Access	71
Configuring the Wireless Guest Network	71
Configuring Advanced Wireless Settings	73
Configuring WDS	76
Configuring WPS	77

### **Chapter 4: Configuring the Firewall** **80**

Cisco RV110W Firewall Features	80
Configuring Basic Firewall Settings	81
Configuring Remote Management	84
Configuring Universal Plug and Play	85
Managing Firewall Schedules	85

Configuring Services Management	86
Configuring Access Rules	87
Adding Access Rules	88
Creating an Internet Access Policy	90
Adding or Editing an Internet Access Policy	90
Configuring Port Forwarding	92
Configuring Single Port Forwarding	92
Configuring Port Range Forwarding	93
Configuring Port Range Triggering	94

## **Chapter 5: Configuring VPN 96**

VPN Tunnel Types	96
VPN Clients	97
Configuring PPTP	97
Configuring NetBIOS Over VPN	98
Creating and Managing PPTP Users	98
Creating and Managing QuickVPN Users	99
Importing VPN Client Settings	100
Configuring Basic VPN Settings (Site-to-Site VPN)	101
Viewing Default Values	102
Configuring Advanced VPN Parameters	103
Managing IKE Policies	103
Configuring Certificate Management	109
Configuring VPN Passthrough	110

## **Chapter 6: Configuring Quality of Service (QoS) 112**

Configuring Bandwidth Management	112
Configuring QoS Port-Based Settings	114
Configuring CoS Settings	115
Configuring DSCP Settings	115

<b>Chapter 7: Administering Your Cisco RV110W</b>	<b>117</b>
Setting Password Complexity	117
Configuring User Accounts	118
Setting the Session Timeout Value	119
Configuring Simple Network Management (SNMP)	120
Using Diagnostic Tools	122
Network Tools	122
Configuring Port Mirroring	124
Configuring Logging	124
Configuring Logging Settings	124
Configuring the E-Mailing of Logs	126
Configuring Bonjour	128
Configuring Date and Time Settings	128
Backing Up and Restoring the System	129
Upgrading Firmware or Change the Language	132
Restarting the Cisco RV110W	133
Restoring the Factory Defaults	134
Running the Setup Wizard	134
<b>Chapter 8: Viewing the Cisco RV110W Status</b>	<b>137</b>
Viewing the Dashboard	137
Viewing the System Summary	139
Viewing the Wireless Statistics	141
Viewing the VPN Status	142
Viewing the IPSec Connection Status	143
Viewing Logs	144
Viewing Connected Devices	145
Viewing Port Statistics	146
Viewing the GuestNet Status	147

<b>Appendix A: Using Cisco QuickVPN</b>	<b>149</b>
Overview	149
Before You Begin	149
Installing the Cisco QuickVPN Software	150
Installing from the CD-ROM	150
Downloading and Installing from the Internet	152
Using the Cisco QuickVPN Software	152
<b>Appendix B: Where to Go From Here</b>	<b>154</b>

# Introduction

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

- **Product Overview**
- **Getting to Know the Cisco RV110W**
- **Installing the Cisco RV110W**
- **Connecting the Equipment**
- **Using the Setup Wizard**
- **Verifying the Hardware Installation**
- **Connecting to Your Wireless Network**

## Product Overview

Thank you for choosing the Cisco RV110W Wireless-N VPN Firewall.

The Cisco RV110W 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 RV110W provides a Wireless-N access point, combined with support for Virtual Private Network (VPN) clients to make remote access to your network more secure.

The router 10/100 Fast Ethernet WAN interface connects directly to your broadband DSL or Cable modem.



## LAN Ethernet Interfaces

The Cisco RV110W provides four full-duplex 10/100 Fast Ethernet LAN interfaces that can connect up to four devices. You can connect a Cisco switch to one of the available ports to expand your network as needed.

## Wireless Access Point

The Cisco RV110W wireless access point supports the 802.11n standard with MIMO technology, which multiplies the effective data rate. This technology results in better throughput and coverage than that provided by 802.11g networks.

## Firewall and VPN Client Access

The Cisco RV110W 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 RV110W supports up to five client-to-gateway VPN tunnels to facilitate branch office connectivity through encrypted virtual links. Users connecting through a VPN tunnel are attached to your company network with secure access to files, e-mail, and your intranet as if they were in the building.

## Security

The Cisco RV110W implements WPA Personal, WPA Enterprise, WPA2 personal, WPA2 Enterprise, and WEP Security, 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 RV110W supports Wi-Fi Multimedia (WMM) and Wi-Fi Multimedia Power Save (WMM-PS) for Quality of Service (QoS).

The Cisco RV110W also 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.

## Wireless Distribution System

The Cisco RV110W wireless access point supports Wireless Distribution System (WDS), which allows the wireless coverage to be expanded without wires.

## Virtual Networks

The Cisco RV110W also supports multiple Service Set Identifiers (SSIDs) for the use of virtual networks (up to four separate virtual networks), with 802.1Q-based VLAN support for traffic separation.

## Configuration and Administration



With the Cisco RV110W embedded web server, you can configure the Cisco RV110W settings using the browser-based Device Manager. The Cisco RV110W supports Internet Explorer, Firefox, and Safari web browsers.





The Cisco RV110W also provides a Setup Wizard that allows you to easily and quickly configure the Cisco RV110W basic settings.

# Getting to Know the Cisco RV110W

## Front Panel



	<b>Power</b>	The Power light is green to indicate the unit is powered on. The light flashes green when the power is coming on.
	<b>WPS</b>	The Wi-Fi Protected Setup (WPS) button is used to configure wireless access for devices in your network that are WPS-enabled. See <a href="#">Configuring WPS</a> for more information.

	<b>Power</b>	The Power light is green to indicate the unit is powered on. The light flashes green when the power is coming on.
	<b>WAN</b>	The WAN (Internet) light is green when the Cisco RV110W is connected to the Internet through your cable or DSL modem. The light is off when the Cisco RV110W is not connected to the Internet. The light flashes green when it is sending or receiving data.
	<b>Wireless</b>	The Wireless light is green when the wireless module is enabled. The light is off when the wireless module is disabled. The light flashes green when the firewall is transmitting or receiving data on the wireless module.
	<b>LAN Ports</b>	<p>The numbered lights correspond to the LAN ports on the Cisco RV110W.</p> <p>If the lights are continuously green, the Cisco RV110W is connected to a device through the corresponding port (1, 2, 3, or 4). The light for a port flashes green when the firewall is actively sending or receiving data over that port.</p>

## Back Panel



<b>RESET</b>	<p>If the Cisco RV110W has problems connecting to the Internet, press the <b>RESET</b> button for at least 3 but no more than 10 seconds with a paper clip or similar object. This is similar to pressing the reset button on your PC to reboot it.</p> <p>If you are experiencing extreme problems with the Cisco RV110W and have tried all other troubleshooting measures, press and hold in the <b>RESET</b> button for more than 10 seconds. This reboots the unit and restores the factory defaults. Changes you have previously made to the Cisco RV110W settings are lost.</p>
<b>LAN (1–4)</b>	LAN connections to network devices, such as PCs, print servers, or switches.
<b>WAN</b>	The WAN (Internet) port is connected to your Internet device, such as a cable or DSL modem.
<b>POWER</b>	Press to turn the Cisco RV110W on or off.
<b>12VDC</b>	Connect the provided 12V AC power adapter to the 12VDC port.

## Installing the Cisco RV110W

### Placement Tips

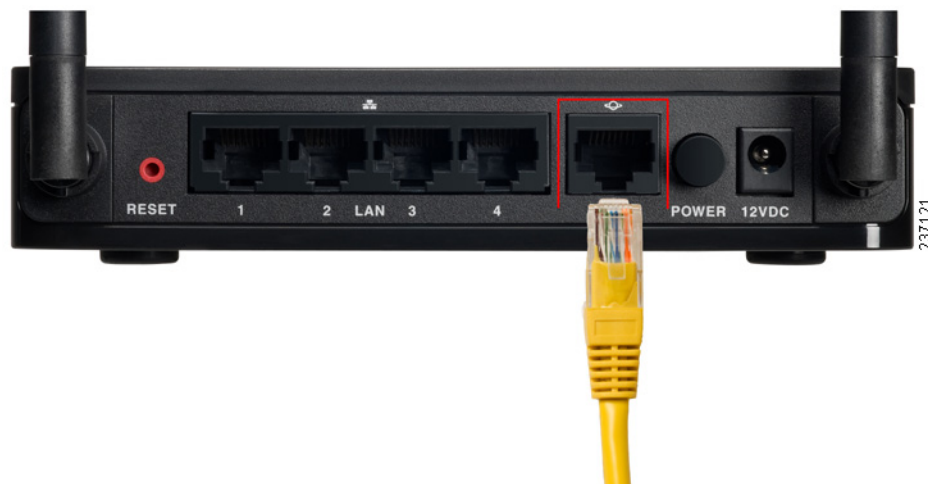
- **Ambient Temperature**—To prevent the firewall from overheating, do not operate it in an area that exceeds an ambient temperature of 104°F (40°C).
- **Air Flow**—Be sure that there is adequate air flow around the firewall.
- **Mechanical Loading**—Be sure that the firewall is level and stable to avoid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

Place the Cisco RV110W horizontally on a flat surface so that it sits on its rubber feet.

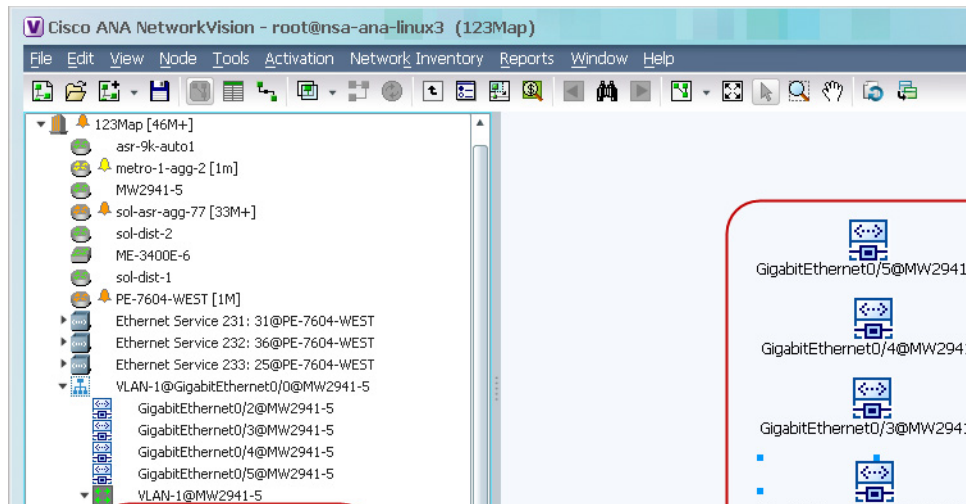
## Connecting the Equipment

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

- STEP 1** Power off all equipment, including the cable or DSL modem, the PC, and the Cisco RV110W.
- STEP 2** You should already have an Ethernet cable connecting your PC to your current cable or DSL modem. Unplug one end of the cable from your PC and plug it into the port marked “WAN” on the unit.



- STEP 3** Connect one end of a different Ethernet cable to one of the LAN (Ethernet) ports on the back of the unit. (In this example, the LAN 1 port is used.) Connect the other end to an Ethernet port on the PC that you will use to run the web-based Setup Wizard and Device Manager.

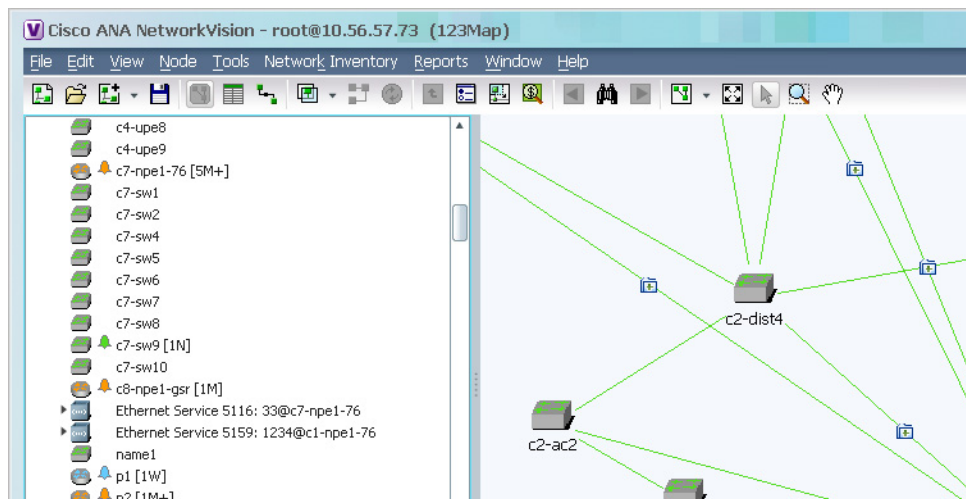


- STEP 4** Power on the cable or DSL modem and wait until the connection is active.

- STEP 5** Connect the power adapter to the Cisco RV110W power port (12VDC).



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



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

**STEP 7** On the Cisco RV110W, push the **POWER** button in to turn on the firewall.

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



## Using the Setup Wizard

The Setup Wizard and Device Manager are supported on Microsoft Internet Explorer 6.0 or later, Mozilla Firefox 3.0 or later, and Apple Safari 3.0 or later.

To use the Setup Wizard:

**STEP 1** Start the computer that you connected to the LAN1 port in Step 2 of the **Connecting the Equipment** section.

Your computer becomes a DHCP client of the Cisco RV110W 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 bar. This is the default IP address of the Cisco RV110W.

A message appears about the site security certificate. The Cisco RV110W uses a self-signed security certificate and this message appears because the Cisco RV110W is not known to your computer.

**STEP 3** Click **Continue to this website** (or the option shown on your particular web browser) to go to the web site.

**STEP 4** When the login page appears, enter the user name and password.

The default user name is **cisco**. The default password is **cisco**. Passwords are case sensitive.

**STEP 5** Click **Log In**. The Setup Wizard starts.

**STEP 6** Follow the on-screen instructions to set up the Cisco RV110W.

The Setup Wizard tries to automatically detect and configure your connection. If it cannot, the Setup Wizard may ask you for information about your Internet connection. You may need to contact your ISP to obtain this information.

**NOTE:** When using the Setup Wizard, you can only set up one wireless network, or SSID. The Cisco RV110W supports up to four wireless networks. If you want to configure additional wireless networks, use the web-based Device Manager. See [Configuring the Wireless Network](#).

After the Setup Wizard is done configuring the Cisco RV110W, you are required to change the default password. We recommend that you use password complexity; see [Setting Password Complexity](#).

After changing the default password, the **Getting Started** page appears. See [Using the Getting Started Page](#) for more information.

## Using the Getting Started Page

The **Getting Started** page displays the most common Cisco RV110W 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 on start up** at the bottom of the page.



## Initial Settings

<b>Change Default Administrator Password</b>	Click to open the <b>Users</b> page where you can change the administrator password. See <a href="#">Configuring User Accounts</a> .
<b>Launch Setup Wizard</b>	Click to launch the Setup Wizard.
<b>Configure WAN Settings</b>	Click to open the <b>Internet Setup</b> page. See <a href="#">Configuring the WAN Settings</a> .
<b>Configure LAN Settings</b>	Click this link to open the <b>LAN Configuration</b> page. See <a href="#">Configuring the LAN Settings</a> .
<b>Configure Wireless Settings</b>	Click to open the <b>Basic Settings</b> page. See <a href="#">Configuring Basic Wireless Settings</a> .

## Quick Access

<b>Upgrade Router Firmware</b>	Click to open the <b>Firmware/Language Upgrade</b> page. See <a href="#">Upgrading Firmware or Change the Language</a> .
<b>Add VPN Clients</b>	Click to open the <b>VPN Clients</b> page. See <a href="#">VPN Clients</a> .
<b>Configure Remote Management Access</b>	Click to open the <b>Basic Settings</b> page. See <a href="#">Configuring Basic Firewall Settings</a> .

## Device Status

<b>System Summary</b>	Click to open the <b>System Summary</b> page. See <a href="#">Viewing the System Summary</a> .
<b>Wireless Status</b>	Click to open the <b>Wireless Statistics</b> page. See <a href="#">Viewing the Wireless Statistics</a> .
<b>VPN Status</b>	Click to open the <b>VPN Status</b> page. See <a href="#">Viewing the VPN Status</a> .

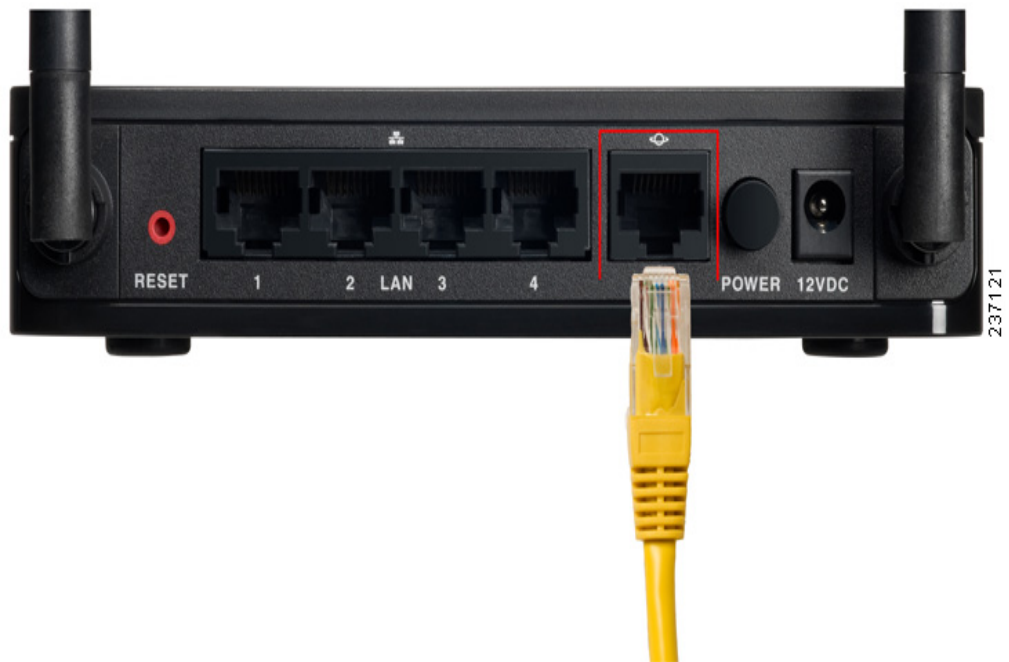
**Other Resources**

<b>Support</b>	Click to open the Cisco support page.
<b>Forums</b>	Click to visit Cisco 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. Under it, click a menu name to perform an action or display a sub-menu.



## Saving 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.

## Configuration Next Steps

Although the Setup Wizard automatically configures the Cisco RV110W, we recommend that you change some default settings to provide better security and performance.

In addition, you may need to manually configure some settings. A suggested outline of steps follows:

1. Change the idle timeout value—By default, The Device Manager logs you out after 10 minutes of inactivity. This can be frustrating if you are trying to configure your device. See [Setting the Session Timeout Value](#).
2. (Optional) If you already have a DHCP server on your network, and you do not want the Cisco RV110W to act as a DHCP server, see [Configuring the LAN Settings](#).
3. Configure your wireless network, especially wireless security. See [Configuring the Wireless Network](#)
4. Configure your Virtual Private Network (VPN) using QuickVPN. The QuickVPN software is found on the documentation and software CD that shipped with your firewall. See [Using Cisco QuickVPN](#)

## Verifying the Hardware Installation

To verify the hardware installation, complete the following tasks:

- Check the LED states. They are described in [Getting to Know the Cisco RV110W](#).
- Connect a computer to an available LAN port and verify that you can connect to a website on the Internet, such as [www.cisco.com](http://www.cisco.com).

- Configure a device to connect to your wireless network and verify the wireless network is functional. See [Connecting to Your Wireless Network](#).

## Connecting to Your Wireless Network

To connect a device (such as a computer) to your wireless network, configure the wireless connection on the device with the wireless security information you configured for the Cisco RV110W by using the Setup Wizard.

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

---

**STEP 1** Open the wireless connection settings window or program for your device.

Your computer may have special software installed to manage wireless connections, or you may find wireless connections under the Control Panel in the **Network Connections** or **Network and Internet** window. (The location depends on your operating system.)

**STEP 2** Enter the network name (SSID) you chose for your network in the Setup Wizard.

**STEP 3** Choose the type of encryption and enter the security key that you specified in the Setup Wizard.

If you did not enable security (not recommended), leave the wireless encryption fields that were configured with the security type and passphrase blank.

**STEP 4** Verify your wireless connection and save your settings.

---



# Configuring Networking

## Configuring the WAN Settings

Configuring WAN properties for an IPv4 network differs depending on which type of Internet connection you have.

### Configuring Automatic Configuration (DHCP)

If your Internet Service Provider (ISP) uses the Dynamic Host Control Protocol (DHCP) to assign you an IP address, you receive a dynamic IP address that is newly generated each time you log in.

To configure DHCP WAN settings:

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

<b>Internet IP Address</b>	Enter the IP address of the WAN port.
<b>Subnet mask</b>	Enter subnet mask of the WAN port.

<b>Default Gateway</b>	Enter the IP address of the default gateway.
<b>Static DNS 1</b>	Enter the IP address of the primary DNS server.
<b>Static DNS 2</b>	Enter the IP address of the secondary DNS server.

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

### Configuring PPPoE

To configure the PPPoE settings:

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

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

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

<b>Username</b>	Enter your username assigned to you by the ISP.
<b>Password</b>	Enter your password assigned to you by the ISP.
<b>Connect on Demand</b>	Select this option if your ISP charges based on the amount of time that you are connected. When you select this option, the Internet connection is on only when traffic is present. If the connection is idle—that is, no traffic is flowing—the connection is closed. If you click <b>Connect on Demand</b> , enter the number of minutes after which the connection shuts off in the <b>Max Idle Time</b> field.
<b>Keep alive</b>	When you select this option, the Internet connection is always on. In the redial period field, enter the number of seconds after which the Cisco RV110W attempts to reconnect if it is disconnected.

<b>Authentication Type</b>	<p>Choose the authentication type:</p> <p><b>Auto-negotiation</b>—The server sends a configuration request specifying the security algorithm set on it. Then, the Cisco RV110W sends back authentication credentials with the security type sent earlier by the server.</p> <p><b>PAP</b>—The Cisco RV110W uses the Password Authentication Protocol (PAP) to connect to the ISP.</p> <p><b>CHAP</b>—The Cisco RV110W uses the Challenge Handshake Authentication Protocol (CHAP) when connecting with the ISP.</p> <p><b>MS-CHAP or MS-CHAPv2</b>—The Cisco RV110W uses Microsoft Challenge Handshake Authentication Protocol when connecting with the ISP.</p>
----------------------------	--

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

### Configuring PPTP

To configure the PPTP settings:

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

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

**STEP 3** Enter this information:

<b>Internet IP Address</b>	Enter the IP address of the WAN port.
<b>Subnet mask</b>	Enter subnet mask of the WAN port.
<b>Default Gateway</b>	Enter the IP address of the default gateway.
<b>PPTP Server</b>	Enter the IP address of the PPTP server.
<b>Username</b>	Enter your username assigned to you by the ISP.
<b>Password</b>	Enter your password assigned to you by the ISP.



<b>Connect on Demand</b>	Select this option if your ISP charges based on the amount of time that you are connected. When you select this option, the Internet connection is on only when traffic is present. If the connection is idle—that is, no traffic is flowing—the connection is closed. If you click <b>Connect on Demand</b> , enter the number of minutes after which the connection shuts off in the <b>Max Idle Time</b> field.
<b>Keep alive</b>	When you select this option, the Internet connection is always on. In the redial period field, enter the number of seconds after which the Cisco RV110W attempts to reconnect if it is disconnected.
<b>Authentication Type</b>	Choose the authentication type:  <b>Auto-negotiation</b> —The server sends a configuration request specifying the security algorithm set on it. Then, the Cisco RV110W sends back authentication credentials with the security type sent earlier by the server.  <b>PAP</b> —The Cisco RV110W uses the Password Authentication Protocol (PAP) to connect to the ISP.  <b>CHAP</b> —The Cisco RV110W uses the Challenge Handshake Authentication Protocol (CHAP) when connecting with the ISP.  <b>MS-CHAP or MS-CHAPv2</b> —The Cisco RV110W uses Microsoft Challenge Handshake Authentication Protocol when connecting with the ISP.

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

---

### Configuring L2TP

To configure the L2TP settings:

---

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

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

**STEP 3** Enter this information:

<b>Internet IP Address</b>	Enter the IP address of the WAN port.
<b>Subnet mask</b>	Enter subnet mask of the WAN port.
<b>Default Gateway</b>	Enter the IP address of the default gateway.
<b>L2TP Server</b>	Enter the IP address of the L2TP server.
<b>Username</b>	Enter your username assigned to you by the ISP.
<b>Password</b>	Enter your password assigned to you by the ISP.
<b>Connect on Demand</b>	Select this option if your ISP charges based on the amount of time that you are connected. When you select this option, the Internet connection is on only when traffic is present. If the connection is idle—that is, no traffic is flowing—the connection is closed. If you click <b>Connect on Demand</b> , enter the number of minutes after which the connection shuts off in the <b>Max Idle Time</b> field.

<b>Keep alive</b>	When you select this option, the Internet connection is always on. In the redial period field, enter the number of seconds after which the Cisco RV110W attempts to reconnect if it is disconnected.
<b>Authentication Type</b>	Choose the authentication type:  <b>Auto-negotiation</b> —The server sends a configuration request specifying the security algorithm set on it. Then, the Cisco RV110W sends back authentication credentials with the security type sent earlier by the server.  <b>PAP</b> —The Cisco RV110W uses the Password Authentication Protocol (PAP) to connect to the ISP.  <b>CHAP</b> —The Cisco RV110W uses the Challenge Handshake Authentication Protocol (CHAP) when connecting with the ISP.  <b>MS-CHAP or MS-CHAPv2</b> —The Cisco RV110W uses Microsoft Challenge Handshake Authentication Protocol when connecting with the ISP.

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

### Configuring Optional Settings

To configure optional settings:

**STEP 1** In the **Optional Settings** section, configure the following settings:

<b>Host Name</b>	Enter the host name of the Cisco RV110W.
<b>Domain Name</b>	Enter the domain name for your network.

<b>MTU</b>	<p>The Maximum Transmit Unit (MTU) is the size of the largest packet that can be sent over the network.</p> <p>The standard MTU value for Ethernet networks is usually 1500 bytes. For PPPoE connections, the value is 1492 bytes.</p> <p>Unless a change is required by your ISP, Cisco recommends that you choose <b>Auto</b>. The default MTU size is 1500 bytes.</p> <p>If your ISP requires a custom MTU setting, choose <b>Manual</b> and enter the MTU size.</p>
<b>Size</b>	Enter the MTU size.

**STEP 2** Click **Save**.

## Configuring the LAN Settings

The default DHCP and TCP/IP settings work for most applications. If you want another PC on your network to be the DHCP server, or if you want to manually configure the network settings of all of your PCs, disable DHCP.

Also, instead of using a DNS server, which maps Internet domain names (for example, [www.cisco.com](http://www.cisco.com)) to IP addresses, you can use a Windows Internet Naming Service (WINS) server. A WINS server is the equivalent of a DNS server but uses the NetBIOS protocol to resolve hostnames. The Cisco RV110W includes the IP address of the WINS server in the DHCP configuration the Cisco RV110W sends to DHCP clients.

**NOTE** If the Cisco RV110W is connected to a modem or device that has a configured network on the same subnet (192.168.1.x), the Cisco RV110W automatically changes the LAN subnet to a random subnet based on 10.x.x.x, so there is no conflict with the subnet on the WAN side of the Cisco RV110W.

You can assign an IP address to each additional subnet on the Cisco RV110W.

## Changing the Default Cisco RV110W IP Address

To configure the default LAN IP address of the Cisco RV110W:

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

**STEP 2** In the **IPv4** section, enter this information:

<b>VLAN</b>	Choose the VLAN number from the drop-down menu.
<b>Local IP Address</b>	Enter the LAN IP address of the Cisco RV110W. Make sure the address is not in use by another device.
<b>Subnet mask</b>	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 RV110W LAN IP address, your PC is no longer connected to the Cisco RV110W.

**STEP 4** To reconnect your PC to the Cisco RV110W, do one of the following:

- If DHCP is configured on the Cisco RV110W, release and renew your PC IP address.
- Manually assign an IP address to your PC. The address must be on the same subnet as the Cisco RV110W. For example, if you change the Cisco RV110W IP address to 10.0.0.1, assign your PC an IP address in the range of 10.0.0.2 to 10.0.0.255.

**STEP 5** Open a new browser window and enter the new IP address of the Cisco RV110W to reconnect.

## Configuring DHCP

By default, the Cisco RV110W functions as a DHCP server to the hosts on the Wireless LAN (WLAN) or LAN network, assigns IP addresses, and provides DNS server addresses.

With DHCP enabled, the Cisco RV110W IP address serves as the gateway address to your LAN. The Cisco RV110W assigns IP addresses to network devices on the LAN from a pool of addresses. The Cisco RV110W tests each address before it is assigned to avoid duplicate addresses on the LAN.

By default the Cisco RV110W assigns an IP address to each host on the LAN from the default IP address pool (192.168.1.100 to 192.168.1.149). If you need to set any host with a static IP address, use an IP address from the 192.168.1.2 to 192.168.1.99 IP address pool. This prevents conflicts with the default IP address pool.

To configure DHCP settings:

- STEP 1** Choose **Networking > LAN > LAN Configuration**.
- STEP 2** (Optional) Select the VLAN you want to edit from the drop-down list.
- STEP 3** In the **DHCP Server** field, select one of the following options:

<b>Enable</b>	Click this button to allow the Cisco RV110W to act as the DHCP server in the network.
<b>Disable</b>	Click this button to disable DHCP on the Cisco RV110W.  If you want another device on your network to be the DHCP server, or to manually configuring the network settings of all of your PCs, disable DHCP.
<b>DHCP Relay</b>	Click this button to select <b>DHCP Relay</b> to configure the Cisco RV110W to act as a relay of IP addresses by a different DHCP server.

**STEP 4** If you selected **Enable**, enter this information:

<b>Starting IP Address</b>	Enter the first address in the IP address pool. Any new DHCP client joining the LAN is assigned an IP address in this range (the ending IP address in the pool is determined by the value you enter in the <b>Maximum Number of DHCP Users</b> field).
<b>Maximum Number of DHCP Users</b>	Enter the maximum number of DHCP clients.
<b>IP Address Range</b>	(Read-only) Displays the range of IP addresses available to the DHCP clients.
<b>Client Lease time</b>	Enter the duration (in hours) for which IP addresses are leased to clients.
<b>Static DNS 1</b>	Enter the IP address of the primary DNS server.
<b>Static DNS 2</b>	Enter the IP address of the secondary DNS server.
<b>Static DNS 3</b>	Enter the IP address of the tertiary DNS server.
<b>WINS</b>	Enter the IP address of the primary WINS server.

**STEP 5** If you selected **DHCP Relay**, enter the address of the relay gateway in the **Remote DHCP Server** field. The relay gateway transmits DHCP messages between multiple subnets.

**STEP 6** Click **Save**.

## Configuring VLANs

A Virtual LAN (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.

The Cisco RV110W has a default VLAN (VLAN 1), which cannot be edited or changed. You can create four other VLANs on the Cisco RV110W.

To create a VLAN:

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

**STEP 2** Click **Add Row**.

**STEP 3** Enter this information:

<b>VLAN ID</b>	Enter the numerical VLAN ID to assign to endpoints in the VLAN membership. The number you enter must be between 3 to 4094. VLAN ID 1 is reserved for the default VLAN, which is used for untagged frames received on the interface. VLAN IDs 1 and 2 are reserved and cannot be used.
<b>Description</b>	Enter a description to identify the VLAN.
<b>Port 1</b>	You can associate VLANS on the Cisco RV110W to the LAN ports on the device. By default, all 4 ports belong to VLAN1. You can edit these ports to associate them with other VLANS. Choose the outgoing frame type for each port:  <b>Untagged</b> —The interface is an untagged member of the VLAN. Frames of the VLAN are sent untagged to the port VLAN.  <b>Tagged</b> —The port is a tagged member of the VLAN. Frames of the VLAN are sent tagged to the port VLAN.  <b>Excluded</b> —The port is currently not a member of the VLAN. This is the default for all the ports when the VLAN is first created.
<b>Port 2</b>	
<b>Port 3</b>	
<b>Port 4</b>	

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

To edit the settings of a VLAN, select the VLAN and click **Edit**. To delete a selected VLAN, click **Delete**. Click **Save** to apply changes.



## Configuring Static DHCP

You can configure the Cisco RV110W to assign a specific IP address to a device with a specific MAC address.

To configure static DHCP:

- STEP 1** Choose **Networking > LAN > Static DHCP**.
- STEP 2** From the **VLAN** drop-down menu, choose a VLAN number.
- STEP 3** Click **Add Row**.
- STEP 4** Enter this information:

<b>Description</b>	Enter a description of the client.
<b>IP Address</b>	Enter the IP address of the device.  The IP address assigned should be outside the pool of the DHCP addresses configured. The DHCP pool is treated as a generic pool and all reserved IP addresses should be outside this pool.  Static DHCP assignment means the DHCP server assigns the same IP to the defined MAC address every time the device is connected to the network.  The DHCP server serves the reserved IP address when the device using the corresponding MAC address requests an IP address.
<b>MAC Address</b>	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).

To edit the settings of a static DHCP client, select the client and click **Edit**. To delete a selected DHCP client, click **Delete**. Click **Save** to apply changes.

---

## Viewing DHCP Leased Clients

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

To view the DHCP clients, choose **Networking > LAN > DHCP Leased Clients**.

For every VLAN defined on the Cisco RV110W, a table displays a list of the clients associated with the VLAN.

To assign a static IP address to one of the connected devices:

---

**STEP 1** In the row of the connected device, check the **Add to Static DHCP** box.

**STEP 2** Click **Save**.

The DHCP server on the Cisco RV110W will then always assign the IP address shown when the device requests an IP address.

---

## Configuring a DMZ Host

The Cisco RV110W supports demilitarized zones (DMZ). A DMZ is a subnetwork that is open to the public but behind the firewall. A DMZ allows you to redirect packets going to your WAN port IP address to a particular IP address in your LAN.

We recommend that you place hosts that must be exposed to the WAN (such as web or e-mail servers) in the DMZ network. You can configure firewall rules to allow access to specific services and ports in 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.

You must configure a fixed (static) IP address for the endpoint that you designate as the DMZ host. You should assign the DMZ host an IP address in the same subnet as the Cisco RV110W LAN IP address, but it cannot be identical to the IP address given to the LAN interface of this gateway.

To configure DMZ:

---

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

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

- STEP 3** From the VLAN drop-down menu, choose the ID of the VLAN where DMZ is enabled.
- STEP 4** In the **Host IP Address** field, enter the IP address of the DMZ host. The DMZ host is the endpoint that receives the redirected packets.
- STEP 5** Click **Save**.

## Configuring RSTP

Rapid Spanning Tree Protocol (RSTP) is a network protocol prevents loops in the network and dynamically reconfigures which physical links should forward frames. To configure Rapid Spanning Tree Protocol (RTSP):

- STEP 1** Choose **Networking > LAN > RSTP**.
- STEP 2** Configure the following settings:

<b>System Priority</b>	<p>Choose the system priority from the drop-down menu. You can choose from a system priority from 0 to 61440 in increments of 4096. Valid values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 40960, 45056, 49152, 53248, 57344, and 61440.</p> <p>The lower the system priority, the more likely the Cisco RV110W is to become the root in the spanning tree. The default is <b>327688</b>.</p>
<b>Hello Time</b>	<p>The hello time is the time period that the root of the spanning tree waits before sending hello messages. Enter a number from 1 to 10. The default is <b>2</b>.</p>
<b>Max Age</b>	<p>The max age is the time period that the router waits to receive a hello message. If the max age is reached, the router tries to change the spanning tree. Enter a number from 6 to 40. The default is <b>20</b>.</p>

---

<b>Forward Delay</b>	The forward delay is the interval after which an interface changes from the blocking to forwarding state. Enter a number from 4 to 30. The default is <b>15</b> .
<b>Force Version</b>	Select the default protocol version to use. Select <b>Normal</b> (use RSTP) or <b>Compatible</b> (compatible with old STP). The default is <b>Normal</b> .

**STEP 3** In the **Setting Table**, configure the following settings:

<b>Protocol Enable</b>	Check to enable RSTP on the associated port. RSTP is disabled by default.
<b>Edge</b>	Check to specify that the associated port is an edge port (end station). Uncheck to specify that the associated port is a link (bridge) to another STP device. Edge port is enabled by default.
<b>Path Cost</b>	Enter the RSTP path cost for the designated ports. Use 0 for the default value (the Cisco RV110W automatically determines the path value). You can also enter a number from 2 to 200000000.

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

---

## Port Management

You can configure the speed and flow control settings of the Cisco RV110W LAN ports.

To configure port speeds and flow control:

---

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

**STEP 2** Configure this information:

<b>Port</b>	The port number.
<b>Link</b>	The port speed. If no device is connected to the port, this field displays <b>Down</b> .
<b>Mode</b>	Choose from the drop-down menu one of the following port speeds: <ul style="list-style-type: none"><li>▪ <b>Auto Negotiation</b>—The Cisco RV110W and the connected device choose a common speed.</li><li>▪ <b>10Mbps Half</b>—10 Mbps in both directions, but only one direction at a time.</li><li>▪ <b>10Mbps Full</b>—10 Mbps in both directions simultaneously.</li><li>▪ <b>100Mbps Half</b>—100 Mbps in both directions, but only one direction at a time.</li><li>▪ <b>100Mbps Full</b>—100 Mbps in both directions simultaneously.</li></ul>
<b>Flow Control</b>	Check to enable flow control for this port.  Flow control is the process of managing the rate of data transmission between two nodes to prevent a fast sender from outrunning a slow receiver. It provides a mechanism for the receiver to control the transmission speed, so that the receiving node is not overwhelmed with data from the transmitting node.

**STEP 3** Click **Save**.

---

## Cloning the MAC Address

Sometimes, you may need to set the MAC address of the Cisco RV110W WAN port to be the same MAC address as your PC or some other MAC address. This is called MAC address cloning.

For example, some ISPs register your computer NIC card MAC address when the service is first installed. When you place a router behind the cable modem or DSL modem, the MAC address from the Cisco RV110W WAN port is not recognized by the ISP.

In this case, to configure your Cisco RV110W to be recognized by the ISP, clone the MAC address of the WAN port to be the same as your computer MAC address.

To configure a MAC address clone:

- 
- STEP 1** Choose **Networking > MAC Address Clone**.
  - STEP 2** In the **MAC Address Clone** field, check **Enable** to enable MAC address cloning.
  - STEP 3** To set the MAC address of the Cisco RV110W WAN port, do one of the following:
    - To set the MAC address of the WAN port to your PC MAC address, click **Clone My PC's MAC**.
    - To specify a different MAC address, enter it in the **MAC Address** field.
  - STEP 4** Click **Save**.
-

## Configuring Routing

Configure the routing options.

### Configuring the Operating Mode

To configure the Cisco RV110W operating mode:

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

**STEP 2** In the **Operating Mode** field, select one of the following options:

<b>Gateway</b>	(Recommended) Click this button to set the Cisco RV110W to act as a gateway.  Keep this default setting if the Cisco RV110W is hosting your network connection to the Internet and is performing the routing functions.
<b>Router</b>	(For advanced users only) Click this button to set the Cisco RV110W to act as a router.  Select this option if the Cisco RV110W is on a network with other routers.  Enabling the Router mode disables NAT (Network Address Translation) on the Cisco RV110W.

**STEP 3** Click **Save**.

### Configuring Dynamic Routing

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

Dynamic Routing (RIP) enables the Cisco RV110W to automatically adjust to physical changes in the network layout and exchange routing tables with the other routers.

The router determines the network packets' route based on the fewest number of hops between the source and the destination. RIP is disabled by default.

**NOTE** RIP is disabled by default on the Cisco RV110W.

To configure dynamic routing:

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

**STEP 2** Configure the following settings:

<b>RIP</b>	Check <b>Enable</b> to enable RIP. This allows the Cisco RV110W to use RIP to route traffic.
<b>RIP Send Packet Version</b>	Select the RIP Send Packet Version ( <b>RIPv1</b> or <b>RIPv2</b> ).  The version of RIP used to send routing updates to other routers on the network depends on the configuration settings of the other routers. RIPv2 is backward compatible with RIPv1.
<b>RIP Recv Packet Version</b>	Choose the RIP Receive Packet Version.

**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. The Cisco RV110W supports up to 30 static routes.

Be careful not to introduce routing loops in your network.

To configure static routing:

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

**STEP 2** From the **Route Entries** drop-down menu, choose a route entry.



To delete the route entry, click **Delete This Entry**.

**STEP 3** Configure the following settings for the selected route entry:

<b>Enter Route Name</b>	Enter the name of the route.
<b>Destination LAN IP</b>	Enter the IP address of the destination LAN.
<b>Subnet Mask</b>	Enter the subnet mask of the destination network.
<b>Gateway</b>	Enter the IP address of the gateway used for this route.
<b>Interface</b>	<p>Select the interface to which packets for this route are sent:</p> <ul style="list-style-type: none"> <li>▪ <b>LAN &amp; Wireless</b>—Click this button to direct packets to the LAN and wireless network.</li> <li>▪ <b>Internet (WAN)</b>—Click this button to direct packets to the Internet (WAN).</li> </ul>

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

### Configuring Inter-VLAN Routing

Check the Inter-VLAN Routing box to enable routing between the separate VLANs on the Cisco RV110W.

## Viewing the Routing Table

The routing table contains information about the topology of the network immediately around it.

To view the routing information on your network, choose **Networking > Routing Table** and choose one of the following:

- **Show IPv4 Routing Table**—The routing table is displayed with the fields configured in the **Networking > Routing** page.
- **Show IPv6 Routing Table**—The routing table is displayed with the fields configured in the **Networking > IPv6** pages.

## Configuring Dynamic DNS

Dynamic DNS (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, TZO.com, 3322.org, or noip.com.

The router notifies 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** From the **DDNS Service** drop-down menu, choose **Disable** to disable this service or choose the DDNS service to use.
- STEP 3** If you do not have a DDNS account, click the URL of the service to visit the selected DDNS service's website so that you can create an account.
- STEP 4** Configure this information:

<b>E-mail Address</b>	(TZO.com and noip.com) Enter the email address you used to create the DDNS account.
<b>Username</b>	(DynDNS.com and 3322.org) Enter the username of the DDNS account.
<b>Password</b>	Enter the password of the DDNS account.
<b>Verify Password</b>	(TZO.com, DynDNS.com, and noip.com) Reenter the password of the DDNS account.
<b>Host Name</b>	(DynDNS.com, 3322.org, and noip.com) Enter the host name of the DDNS server.
<b>Domain Name</b>	(TZO.com) Enter the name of the domain that is used to access the network.

<b>Internet IP Address</b>	(Read-only) The Internet IP address of the Cisco RV110W.
<b>Status</b>	(Read-only) Status is displayed if the DDNS update has completed successfully or if the account update information sent to the DDNS server failed.

**STEP 5** To test the DDNS configuration, click **Test Configuration**.

**STEP 6** Click **Save**.

## Configuring the IP Mode

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

To select an IP mode:

**STEP 1** Choose **Networking > IP Mode**.

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

<b>LAN:IPv4, WAN:IPv4</b>	Choose this option to use IPv4 in the LAN and WAN ports.
<b>LAN:IPv6, WAN:IPv4</b>	Choose this option to use IPv6 in the LAN ports and IPv4 in the WAN ports.
<b>LAN:IPv6, WAN:IPv6</b>	Choose this option to use IPv6 in the LAN and WAN ports.
<b>LAN:IPv4+IPv6, WAN:IPv4</b>	Choose this option to use IPv4 and IPv6 in the LAN ports and IPv4 in the WAN ports.
<b>LAN:IPv4+IPv6, WAN:IPv4+IPv6</b>	Choose this option to use IPv4 and IPv6 in both the LAN and WAN ports.
<b>LAN:IPv4, WAN:IPv6</b>	Choose this option to use IPv4 in the LAN and IPv6 in the WAN ports.

**STEP 3** (Optional) If you are using 6to4 tunneling, which allows IPv6 packets to be transmitted over an IPv4 network, do the following:

- a. Click **Show Static 6to4 DNS Entry**.
- b. In the **Domain** and **IP** fields, enter up to five domain-to-IP mappings.

The 6to4 tunneling feature is typically used when a site or end user wants to connect to the IPv6 Internet using the existing IPv4 network.

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

## Configuring IPv6

Internet Protocol version 6 (IPv6) is a version of the Internet Protocol (IP) intended to succeed Internet Protocol version 4 (IPv4). Configuring WAN properties for an IPv6 network depends on the type of internet connection that you have.

### Configuring the WAN for an IPv6 Network

You can configure the Cisco RV110W to be a DHCPv6 client of the ISP for this WAN or to use a static IPv6 address provided by the ISP.

#### Setting the IP Mode

To configure IPv6 WAN settings on your Cisco RV110W, you must first set the IP mode to LAN:IPv6, WAN:IPv6 or LAN:IPv4+IPv6, WAN:IPv4+IPv6.

See [Configuring the IP Mode](#) for more information.

#### Configuring DHCPv6

If your ISP provides you with a dynamically-assigned address, configure the Cisco RV110W to use be a DHCPv6 client.

To configure the Cisco RV110W to be a DHCPv6 client:

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

**STEP 2** In the **WAN Connection Type** field, select **Automatic Configuration-DHCPv6**.

**STEP 3** Click **Save**.

**Configuring a Static WAN IP Address**

If your ISP assigns you a fixed address to access the Internet, configure the Cisco RV110W to use a static IPv6 address.

To configure the Cisco RV110W to use a static IPv6 address:

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

**STEP 2** In the **WAN Connection Type** field, select **Static IPv6**.

**STEP 3** Enter this information:

<b>IPv6 Address</b>	Enter the IPv6 address of the WAN port.
<b>IPv6 Prefix Length</b>	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 2001:0DB8:AC10:FE01:: IP address, 2001 is the prefix.  All hosts in the network have identical initial bits for their IPv6 address; you set the number of common initial bits in the network addresses in this field.
<b>Default IPv6 Gateway</b>	Enter the IPv6 address of the default gateway. This is the IP address of the server at the ISP that this router connects to for accessing the Internet.
<b>Static DNS 1</b>	Enter the IP address of the primary DNS server on the ISP IPv6 network.
<b>Static DNS 2</b>	Enter the IP address of the secondary DNS server on the ISP IPv6 network.

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

### Configuring PPPoE IPv6 Settings

If you choose this option, your IPv6 WAN PPPoE settings must match your IPv4 WAN PPPoE settings. See [Configuring PPPoE](#).

To configure the Cisco RV110W PPPoE IPv6 settings:

- STEP 1** Choose **Networking > IPv6 > IPv6 WAN Configuration**.
- STEP 2** In the **WAN Connection Type** field, choose **PPPoE IPv6**.
- STEP 3** Enter the following information (you may need to contact your ISP to obtain your PPPoE login information):

<b>Username</b>	Enter your username assigned to you by the ISP.
<b>Password</b>	Enter your password assigned to you by the ISP.
<b>Connect on Demand</b>	Select this option if your ISP charges based on the amount of time that you are connected. When you select this option, the Internet connection is on only when traffic is present. If the connection is idle—that is, no traffic is flowing—the connection is closed. If you click <b>Connect on Demand</b> , enter the number of minutes after which the connection shuts off in the <b>Max Idle Time</b> field.
<b>Keep alive</b>	When you select this option, the Internet connection is always on. In the redial period field, enter the number of seconds after which the Cisco RV110W attempts to reconnect if it is disconnected.

<b>Authentication Type</b>	<p>Choose the authentication type:</p> <p><b>Auto-negotiation</b>—The server sends a configuration request specifying the security algorithm set on it. Then, the Cisco RV110W sends back authentication credentials with the security type sent earlier by the server.</p> <p><b>PAP</b>—The Cisco RV110W uses the Password Authentication Protocol (PAP) to connect to the ISP.</p> <p><b>CHAP</b>—The Cisco RV110W uses the Challenge Handshake Authentication Protocol (CHAP) when connecting with the ISP.</p> <p><b>MS-CHAP or MS-CHAPv2</b>—The Cisco RV110W uses Microsoft Challenge Handshake Authentication Protocol when connecting with the ISP.</p>
<b>Service Name</b>	<p>Your ISP may configure a service name that is needed to log onto the PPPoE server. If so, enter it here.</p>
<b>MTU</b>	<p>The Maximum Transmit Unit (MTU) is the size of the largest packet that can be sent over the network.</p> <p>The standard MTU value for Ethernet networks is usually 1500 bytes. For PPPoE connections, the value is 1492 bytes.</p> <p>Unless a change is required by your ISP, Cisco recommends that you choose <b>Auto</b>. The default MTU size is 1500 bytes.</p> <p>If your ISP requires a custom MTU setting, choose <b>Manual</b> and enter the MTU size.</p>
<b>Size</b>	<p>Enter the MTU size.</p>
<b>Address Mode</b>	<p>Choose dynamic or static address mode. If you choose <i>dynamic</i>, enter the IPv6 address in the field below.</p>
<b>IPv6 Prefix Length</b>	<p>If you chose <i>static</i> address mode, enter the IPv6 prefix length field.</p>

<b>Default IPv6 Gateway</b>	Enter the IP address of the default IPv6 gateway.
<b>Static DNS 1</b>	If you chose <i>static</i> address mode, enter the IP address of the primary DNS server.
<b>Static DNS 2</b>	If you chose <i>static</i> address mode, enter the IP address of the secondary DNS server.

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

## Configuring IPv6 LAN Settings

In the IPv6 mode, the LAN DHCP server is enabled by default (similar to the IPv4 mode). The DHCPv6 server assigns IPv6 addresses from configured address pools that use the IPv6 prefix length assigned to the LAN.

### Setting the IP Mode

To configure IPv6 LAN settings on your Cisco RV110W, you must first set the IP mode to one of the following modes:

- LAN:IPv6, WAN:IPv4
- LAN:IPv6, WAN:IPv6
- LAN:IPv4+IPv6, WAN:IPv4
- LAN:IPv4+IPv6, WAN:IPv4+IPv6

See [Configuring the IP Mode](#) for more information.

### Configuring a Static LAN IP Address

To configure IPv6 LAN settings:

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



**STEP 2** Enter the following information to configure the IPv6 LAN address:

<b>IPv6 Address</b>	<p>Enter the IPv6 address of the Cisco RV110W.</p> <p>The default IPv6 address for the gateway is fec0::1 (or FEC0:0000:0000:0000:0000:0000:0001). You can change this 128-bit IPv6 address based on your network requirements.</p>
<b>IPv6 Prefix Length</b>	<p>Enter the IPv6 prefix length.</p> <p>The IPv6 network (subnet) is identified by the initial bits of the address called the prefix. By default, the prefix is 64 bits long.</p> <p>All hosts in the network have the identical initial bits for their IPv6 address; you set the number of common initial bits in the network addresses in this field.</p>

**STEP 3** Click **Save**.

### Configuring DHCPv6 Settings

To configure IPv6 LAN settings:

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

**STEP 2** Enter the following information to configure the DHCPv6 settings:

<b>DHCP Status</b>	<p>Check to enable the DHCPv6 server.</p> <p>If enabled, the Cisco RV110W assigns an IP address within the specified range plus additional specified information to any LAN endpoint that requests DHCP-served addresses.</p>
<b>Domain Name</b>	<p>(Optional) Enter the domain name of the DHCPv6 server.</p>

<p><b>Server Preference</b></p>	<p>Enter the server preference level of this DHCP server.</p> <p>DHCP advertise messages with the highest server preference value to a LAN host are preferred over other DHCP server advertise messages.</p> <p>The default is 255.</p>
<p><b>Static DNS 1</b></p>	<p>Enter the IPv6 address of the primary DNS server on the ISP IPv6 network.</p>
<p><b>Static DNS 2</b></p>	<p>Enter the IPv6 address of the secondary DNS server on the ISP IPv6 network.</p>
<p><b>Client Lease Time</b></p>	<p>Enter the client lease time.</p> <p>Enter the duration (in seconds) for which IPv6 addresses are leased to endpoints on the LAN.</p>

**STEP 3** Click **Save**.

### Configuring IPv6 Address Pools

You can define the IPv6 delegation prefix for a range of IPv6 addresses to be served by the Cisco RV110W 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.

To configure IPv6 Address Pools:

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

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

**STEP 3** Enter this information:

<b>Start Address</b>	Enter the starting IPv6 address of the pool.
<b>End Address</b>	Enter the ending IPv6 address of the pool.
<b>IPv6 Prefix Length</b>	Enter the prefix length.  This field determines the number of common initial bits in the network addresses.

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

To edit the settings of a pool, select the pool and click **Edit**. To delete a selected pool, click **Delete**. Click **Save** to apply changes.

## Configuring IPv6 Static Routing

You can configure static routes to direct packets to the destination network. A static route is a predetermined 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** Choose **Networking > IPv6 > IPv6 Static Routing**.

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

**STEP 3** Enter this information:

<b>Name</b>	Enter the route name.
<b>Destination</b>	Enter the IPv6 address of the destination host or network for this route.
<b>Prefix Length</b>	Enter the number of prefix bits in the IPv6 address that define the destination subnet.
<b>Gateway</b>	Enter the IPv6 address of the gateway through which the destination host or network can be reached.
<b>Interface</b>	Choose the interface for the route from the drop-down menu: <b>LAN</b> , <b>WAN</b> , or <b>6to4</b> .
<b>Metric</b>	Enter 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.
<b>Active</b>	<p>Check to make the route active.</p> <p>When you add a route in an inactive state, it gets listed in the routing table, but is not used by the Cisco RV110W. You can always activate the route later.</p> <p>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, you can enable the route.</p>

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

To edit the settings of a route, select the route and click **Edit**. To delete a selected route, click **Delete**. Click **Save** to apply changes.

---

## Configuring Routing (RIPng)

RIP Next Generation (RIPng) 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 removes these routes from the routing table.

On the Cisco RV110W, RIPng is disabled by default.

To configure RIPng:

- 
- STEP 1** Choose **Networking > IPv6 > Routing (RIPng)**.
  - STEP 2** Check **Enable**.
  - STEP 3** Click **Save**.
- 

## Configuring Tunneling

### 6 to 4 Tunneling

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

To configure 6-to-4 tunneling:

- 
- STEP 1** Select **Networking > IPv6 > Tunneling**.
  - STEP 2** In the **6 to 4 Tunneling** field, check **Enable**.
  - STEP 3** Choose the type of tunneling (**6to4** or **6RD [Rapid Deployment]**).
  - STEP 4** For 6RD Tunneling, choose **auto** or **manual**.
-

**STEP 5** Enter the following information:

- **IPv6 Prefix**
- **IPv6 Prefix Length**
- **Border Relay**
- **IPv4 Mask Length.**

**STEP 6** Click **Save**.

---

### 4 to 6 Tunneling

IPv4 to IPv6 tunneling (4-to-6 tunneling) allows IPv4 packets to be transmitted over an IPv6 network. To configure 4-to-6 tunneling:

---

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

**STEP 2** In the **4 to 6 Tunneling** field, check **Enable**.

**STEP 3** Enter the local WAN IPv6 address on the Cisco RV110W.

**STEP 4** Enter the Remote IPv6 address, or the IP address of the remote endpoint.

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

---

### Viewing IPv6 Tunnel Status

To view IPv6 tunnel status:

---

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

**STEP 2** Click **Refresh** to display the most up-to-date information.

---

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

## Configuring Router Advertisement

The Router Advertisement Daemon (RADVD) on the Cisco RV110W listens for router solicitations in the IPv6 LAN and responds with router advertisements as required. This is stateless IPv6 auto configuration, and the Cisco RV110W distributes IPv6 prefixes to all nodes on the network.

To configure the RADVD:

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

**STEP 2** Enter this information:

<b>RADVD Status</b>	Check <b>Enable</b> to enable RADVD.
<b>Advertise Mode</b>	Select one of the following modes:  <b>Unsolicited Multicast</b> —Select this mode to send Router Advertisements (RAs) to all interfaces belonging to the multicast group.  <b>Unicast only</b> —Select this mode to restrict advertisements to well-known IPv6 addresses only (RAs are sent to the interface belonging to the known address only).
<b>Advertise Interval</b>	If you choose <b>Unsolicited Multicast</b> as the advertise mode, enter the advertise interval (4–1800). The default is <b>30</b> . The advertise interval is a random value between the Minimum Router Advertisement Interval (MinRtrAdvInterval) and Maximum Router Advertisement Interval (MaxRtrAdvInterval).  $\text{MinRtrAdvInterval} = 0.33 * \text{MaxRtrAdvInterval}$
<b>RA Flags</b>	Check <b>Managed</b> to use the administered/stateful protocol for address auto configuration.  Check <b>Other</b> to use the administered/stateful protocol of other, non-address information auto configuration.

<b>Router Preference</b>	<p>Choose <b>low</b>, <b>medium</b>, or <b>high</b> from the drop-down menu. The default is <b>medium</b>.</p> <p>The router preference provides a preference metric for default routers. The low, medium and high values are signaled in unused bits in RA 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.</p>
<b>MTU</b>	<p>Enter the MTU size (0 or 1280 to 1500). The default is <b>1500</b> bytes.</p> <p>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.</p>
<b>Router Life Time</b>	<p>Enter the router lifetime value, or the time in seconds that the advertisement messages exists on the route. The default is <b>3600</b> seconds.</p>

**STEP 3** Click **Save**.

## Configuring Advertisement Prefixes

To configure the RADVD available prefixes:

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

**STEP 2** Click **Add Row**.



**STEP 3** Enter this information:

<b>IPv6 Prefix Type</b>	<p>Choose one of the following types from the drop-down menu:</p> <p><b>6to4</b>—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</p> <p><b>Global/Local</b>—A locally unique IPv6 address that you can use in private IPv6 networks or a globally unique IPv6 Internet address.</p>
<b>SLA ID</b>	<p>If you choose <b>6to4</b> as the IPv6 prefix type, enter the Site-Level Aggregation Identifier (SLA ID).</p> <p>The SLA ID in the 6to4 address prefix is set to the interface ID of the interface on which the advertisements are sent.</p>
<b>IPv6 Prefix</b>	<p>If you choose <b>Global/Local</b> as the IPv6 prefix type, enter the IPv6 prefix. The IPv6 prefix specifies the IPv6 network address.</p>
<b>IPv6 Prefix Length</b>	<p>If you choose <b>Global/Local</b> as the IPv6 prefix type, enter the prefix length. 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.</p>
<b>Prefix Lifetime</b>	<p>Enter the prefix lifetime, or the length of time over which the requesting router is allowed to use the prefix.</p>

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







# Configuring the Wireless Network

## Wireless Security

Wireless networks are convenient and easy to install, so small businesses and homes with high-speed Internet access are adopting them at a rapid pace.

Because wireless networking operates by sending information over radio waves, it can be more vulnerable to intruders than a traditional wired network.

### Wireless Security Tips

You cannot physically prevent someone from connecting to your wireless network, but you can take the following steps to keep your network secure:

- Change the default wireless network name or SSID.

Wireless devices have a default wireless network name or SSID. This is the name of your wireless network, and can be up to 32 characters in length.

To protect your network, change the default wireless network name to a unique name to distinguish your wireless network from other wireless networks that may exist around you.

When choosing names, 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 are asked for a password when you want to change their settings. These devices have a default password. The default password is often **cisco**.

Hackers know these default values and may try to use them to access your wireless device and change your network settings. To thwart unauthorized access, customize the device password so it is hard to guess.

- Enable MAC address filtering.

Cisco routers and gateways give you the ability to enable 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, 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) to prevent applications from using file sharing without your consent.

## Cisco RV110W Wireless Networks

The Cisco RV110W provides four virtual wireless networks, or four SSIDs (Service Set Identifier): ciscosb1, ciscosb2, ciscosb3, and ciscosb4. These are the default names or SSIDs of these networks, but you can change these names to more meaningful names. This table describes the default settings of these networks:

SSID Name	ciscosb1	ciscosb2	ciscosb3	ciscosb4
<b>Enabled</b>	Yes	No	No	No
<b>SSID Broadcast</b>	Enabled	Disabled	Disabled	Disabled
<b>Security Mode</b>	Disabled <sup>1</sup>	Disabled	Disabled	Disabled
<b>MAC Filter</b>	Disabled	Disabled	Disabled	Disabled
<b>VLAN</b>	1	1	1	1
<b>Wireless Isolation with SSID</b>	Disabled	Disabled	Disabled	Disabled
<b>WMM</b>	Enabled	Enabled	Enabled	Enabled
<b>WPS Hardware Button</b>	Enabled	Disabled	Disabled	Disabled

1. When using the Setup Wizard, select **Best Security** or **Better Security** to protect the Cisco RV110W from unauthorized access.

## Configuring Basic Wireless Settings

You can use the **Basic Settings** page (**Wireless > Basic Settings**) to configure basic wireless settings.

To configure basic wireless settings:

- STEP 1** Choose **Wireless > Basic Settings**.
- STEP 2** In the **Radio** field, check **Enable** to turn on the wireless radio. By default there is only one wireless network enabled, **ciscosb1**.
- STEP 3** In the **Wireless Network Mode** field, choose one of these options from the drop-down menu:

<b>B/G/N-Mixed</b>	Choose this option if you have Wireless-N, Wireless-B, and Wireless-G devices in your network. This is the default setting (recommended).
<b>B Only</b>	Choose this option if you have only Wireless-B devices in your network.
<b>G Only</b>	Choose this option if you have only Wireless-G devices in your network.
<b>N Only</b>	Choose this option if you have only Wireless-N devices in your network.
<b>B/G-Mixed</b>	Choose this option if you have Wireless-B and Wireless-G devices in your network.
<b>G/N-Mixed</b>	Choose this option if you have Wireless-G and Wireless-N devices in your network.

- STEP 4** If you chose **B/G/N-Mixed**, **N-Only**, or **G/N Mixed**, in the **Wireless Band Selection** field, select the wireless bandwidth on your network (**20MHz** or **20/40MHz**). If you chose **N-Only**, you must use WPA2 security on your network. See [Configuring the Security Mode](#).
- STEP 5** In the **Wireless Channel** field, choose the wireless channel from the drop-down menu.



**STEP 6** In the **AP Management VLAN** field, choose **VLAN 1** if you are using the default settings.

If you create additional VLANs, choose a value that corresponds with the VLAN configured on other switches in the network. This is done for security purposes. You might need to change the management VLAN to limit access to the Cisco RV110W Device Manager.

**STEP 7** (Optional) In the **U-APSD (WMM Power Save)** field, check **Enable** to enable the Unscheduled Automatic Power Save Delivery (U-APSD) feature, also referred to as WMM Power Save, that allows the radio to conserve power.

U-APSD is a power saving scheme optimized for real-time applications, such as VoIP, transferring full-duplex data over WLAN. By classifying outgoing IP traffic as *Voice* data, these types of applications can increase battery life by approximately 25% and minimize transmit delays.

**STEP 8** (Optional) Configure the settings of the four wireless networks (see [Editing the Wireless Network Settings](#)).

**STEP 9** Click **Save**.

## Editing the Wireless Network Settings

The **Wireless Table** in the **Basic Settings** page (**Wireless > Basic Settings**) lists the settings of the four wireless networks supported on the Cisco RV110W.

To configure wireless network settings:

**STEP 1** Check the box for the networks you want to configure.

**STEP 2** Click the **Edit** button.

**STEP 3** Configure these settings:

<b>Enable SSID</b>	Click <b>On</b> to enable the network.
<b>SSID Name</b>	Enter the name of the network.
<b>SSID Broadcast</b>	Check this box to enable SSID broadcast. If SSID broadcast is enabled, the wireless router advertises its availability to wireless-equipped devices in the range of the router.

<b>VLAN</b>	Choose the VLAN associated with the network.
<b>Wireless Isolation with SSID</b>	Check this box to enable wireless isolation within the SSID.
<b>WMM (Wi-Fi Multimedia)</b>	Check this box to enable WMM.
<b>WPS Hardware Button</b>	Check this box to map the Cisco RV110W WPS button on the front panel to this network.

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

## Configuring the Security Mode

You can configure one of the following security modes for wireless networks:

### Configuring WEP

The WEP security mode offers 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.

**NOTE** If you do not have to use WEP, we recommend that you use WPA2. If you are using the Wireless-N only mode, you must use WPA2.

To configure the WEP security mode:

**STEP 1** In the **Wireless Table (Wireless > Basic Settings)**, check the box for the network you want to configure.

**STEP 2** Click **Edit Security Mode**.

The **Security Settings** page appears.

**STEP 3** In the **Select SSID** field, choose the SSID for which to configure the security settings.

**STEP 4** From the **Security Mode** menu, choose **WEP**.

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

- **Open System**—This is the default option.
- **Shared Key**—Select this option if your network administrator recommends this setting. If you are unsure, select the default option.

In both cases, the wireless client must provide the correct shared key (password) to access the wireless network.

**STEP 6** In the **Encryption** field, choose the encryption type:

- **10/64-bit(10 hex digits)**—Provides a 40-bit key.
- **26/128-bit(26 hex digits)**—Provides a 104-bit key, which offers stronger encryption, making the key more difficult to crack. We recommend 128-bit encryption.

**STEP 7** (Optional) In the **Passphrase** field, enter an alphanumeric phrase (longer than eight characters for optimal security) and click **Generate Key** to generate four unique WEP keys in the WEP Key fields below.

If you want to provide your own key, enter it directly in the **Key 1** field (recommended). The length of the key should be 5 ASCII characters (or 10 hexadecimal characters) for 64-bit WEP and 13 ASCII characters (or 26 hexadecimal characters) for 128-bit WEP. Valid hexadecimal characters are 0 to 9 and A to F.

**STEP 8** In the **TX Key** field, choose which key to use as the shared key that devices must use to access the wireless network.

**STEP 9** Click **Save** to save your settings.

**STEP 10** Click **Back** to go back to the **Basic Settings** page.

---

### Configuring WPA-Personal, WPA2-Personal, and WPA2-Personal Mixed

The WPA Personal, WPA2 Personal, and the WPA2 Personal Mixed security modes offer strong security to replace WEP.

- **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. WPA-Personal supports Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES) encryption.
- **WPA2-Personal**—(Recommended) WPA2 is the implementation of the security standard specified in the final 802.11i standard. WPA2 supports AES encryption and this option uses Preshared Key (PSK) for authentication.
- **WPA2-Personal Mixed**—Allows both WPA and WPA2 clients to connect simultaneously using PSK authentication.

The personal authentication is the PSK that is an alphanumeric passphrase shared with the wireless peer.

To configure the WPA Personal security mode:

- STEP 1** In the **Wireless Table (Wireless > Basic Settings)**, check the box for the network you want to configure.
- STEP 2** Click **Edit Security Mode**. The **Security Settings** page appears.
- STEP 3** In the **Select SSID** field, choose the SSID for which to configure the security settings.
- STEP 4** From the **Security Mode** menu, choose one of the three WPA Personal options.
- STEP 5** (WPA-Personal only) In the **Encryption** field, choose one of the following options:
  - **TKIP/AES**—Choose **TKIP/AES** to ensure compatibility with older wireless devices that may not support AES.
  - **AES**—This option is more secure.
- STEP 6** In the **Security Key** field, enter an alphanumeric phrase (8–63 ASCII characters or 64 hexadecimal digits). The password strength meter shows how secure the key is: below minimum, weak, strong, very strong, or secure. We recommend using a security key that registers on the strength meter as secure.
- STEP 7** To show the security key as you are entering it, check the **Unmask Password** box.
- STEP 8** In the **Key Renewal** field, enter the duration of time (600–7200 seconds) between key renewals. The default value is 3600.
- STEP 9** Click **Save** to save your settings.
- STEP 10** Click **Back** to go back to the **Basic Settings** page.

---

### Configuring WPA-Enterprise, WPA2-Enterprise, and WPA2-Enterprise Mixed

The WPA Enterprise, WPA2 Enterprise, and the WPA2 Enterprise Mixed security modes allow you to use RADIUS server authentication.

- **WPA-Enterprise**—Allows you to use WPA with RADIUS server 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.

To configure the WPA Enterprise security mode:

- STEP 1** In the **Wireless Table (Wireless > Basic Settings)**, check the box for the network you want to configure.
- STEP 2** Click **Edit Security Mode**.
- STEP 3** In the **Select SSID** field, choose the SSID for which to configure the security settings.
- STEP 4** From the **Security Mode** menu, choose one of the three WPA Enterprise options.
- STEP 5** (WPA-Enterprise only) In the **Encryption** field, choose one of the following options:
  - **TKIP/AES**—Choose **TKIP/AES** to ensure compatibility with older wireless devices that may not support AES.
  - **AES**—This option is more secure.
- STEP 6** In the **RADIUS Server** field, enter the IP address of the RADIUS server.
- STEP 7** In the **RADIUS Port** field, enter the port used to access the RADIUS server.
- STEP 8** In the **Shared Key** field, enter an alphanumeric phrase (8–63 ASCII characters or 64 hexadecimal digits).
- STEP 9** In the **Key Renewal** field, enter the duration of time (600–7200 seconds) between key renewals. The default value is 3600.
- STEP 10** Click **Save** to save your settings.
- STEP 11** Click **Back** to go back to the **Basic Settings** page.

---

## 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 computers and only allow those computers to access the network. You can configure MAC Filtering for each network or SSID.

To configure MAC filtering:

- 
- STEP 1** In the **Wireless Table (Wireless > Basic Settings)**, check the box for the network you want to configure.
  - STEP 2** Click **Edit MAC Filtering**. The **Wireless MAC Filter** page appears.
  - STEP 3** In the **Edit MAC Filtering** field, check the **Enable** box to enable MAC Filtering for this SSID.
  - STEP 4** In the **Connection Control** field, choose the type of access to the wireless network:
    - **Prevent**—Select this option to prevent devices with the MAC addresses listed in the **MAC Address Table** from accessing the wireless network. This option is selected by default.
    - **Permit**—Select this option to allow devices with the MAC addresses listed in the **MAC Address Table** to access the wireless network.
  - STEP 5** To show computers and other devices on the wireless network, click **Show Client List**.
  - STEP 6** In the **Save to MAC Address Filter List** field, check the box to add the device to the list of devices to be added to the **MAC Address Table**.
  - STEP 7** Click **Add to MAC** to add the selected devices in the **Client List Table** to the **MAC Address Table**.
  - STEP 8** Click **Save** to save your settings.
  - STEP 9** Click **Back** to go back to the **Basic Settings** page.
-

---

## Configuring Time of Day Access

To further protect your network, you can restrict access to it by specifying when users can access the network.

To configure Time of Day Access:

- 
- STEP 1** In the **Wireless Table (Wireless > Basic Settings)**, check the box for the network you want to configure.
  - STEP 2** Click **Time of Day Access**. The Time of Day Access page appears.
  - STEP 3** In the **Active Time** field, check **Enable** to enable Time of Day Access.
  - STEP 4** In the **Start Time** and **Stop Time** fields, specify the time of day period when access to the network is allowed.
  - STEP 5** Click **Save**.
- 

## Configuring the Wireless Guest Network

The Cisco RV110W supports a wireless “guest” network that is separated from the other wireless SSIDs, or networks, on the router. This router provides secure guest access that is isolated from the rest of the network, and can be configured to restrict access time and bandwidth used. The following restrictions and configuration guidelines apply:

- One guest network can be configured for each Cisco RV110W
- The guest network is configured as one of the four available SSIDs on the Cisco RV110W
- The guest network cannot be configured on the AP Management VLAN (VLAN ID 1).

To configure the guest network:

### Create a new VLAN

- 
- STEP 1** In the Management Interface, choose **Networking > LAN > VLAN Membership**.
  - STEP 2** In the *VLAN Setting Table*, add a new VLAN for the guest network. For example, click **Add Row** and enter the following:
    - **VLAN ID**—Enter a number for the VLAN (for example, 4).

- **Description**—Enter a name for the VLAN (for example, **guest-net**).

**STEP 3** Leave the ports as **tagged** and click **Save**.

---

#### Set up the Guest network:

---

- STEP 1** In the Management Interface, choose **Wireless > Basic Settings**.
- STEP 2** In the *Wireless Table*, choose the SSID or network that you want to designate as the guest network.
- STEP 3** Click **Edit**. Change the SSID name to reflect the “guest” designation (for example, “*guest-net*”).
- STEP 4** Check the *SSID Broadcast* box so that the network will appear as an available wireless connection to clients searching for networks.
- STEP 5** Check the *Guest Network* box to configure this SSID as the guest network.
- STEP 6** Choose the VLAN you created for the guest network (or, if you have not yet created a network, select **Add New VLAN**).
- STEP 7** Click **Save**. The system notifies you that the physical Ethernet ports on the Cisco RV110W are excluded from the VLAN that you have assigned to the guest network. In addition, *Wireless Isolation with SSID* and *WMM* are automatically enabled.
- 

#### Configure the Password and Other Options

---

- STEP 1** In the Management Interface, choose **Wireless > Basic Settings**.
- STEP 2** Under the *Wireless Table*, click **Edit Guest Net**.
- STEP 3** Enter a password that users will enter to access the guest network.
- STEP 4** Enter the password again to confirm.
- STEP 5** Enter the time, in minutes, that the guest connection will be available for users.
- STEP 6** (Optional) To restrict bandwidth usage by the guest network, check *Enable Guest Bandwidth Restriction*. (QoS must be enabled first; click the link to the Bandwidth Management page if you need to configure QoS.) In the *Available Bandwidth* field, enter the percentage of bandwidth to allocate to the guest network.



**STEP 7** Click **Save**.

## Configuring Advanced Wireless Settings

Advanced wireless settings should be adjusted only by an expert administrator; incorrect settings can reduce wireless performance.

To configure advanced wireless settings:

**STEP 1** Choose **Wireless > Advanced Settings**. The Advanced Settings page appears.

**STEP 2** Configure these settings:

<b>Frame Burst</b>	Enable this option to provide your wireless networks with greater performance, depending on the manufacturer of your wireless products. If you are not sure how to use this option, keep the default (enabled).
<b>WMM No Acknowledgement</b>	Click to enable this feature. Enabling WMM No Acknowledgement can result in more efficient throughput, but higher error rates in a noisy Radio Frequency (RF) environment. Default setting is disabled

<b>Basic Rate</b>	<p>The Basic Rate setting is not the rate of transmission but a series of rates at which the Services Ready Platform can transmit. The Cisco RV110W advertises its basic rate to the other wireless devices in your network, so they know which rates will be used. The Services Ready Platform will also advertise that it will automatically select the best rate for transmission.</p> <p>The default setting is Default, when the Cisco RV110W can transmit at all standard wireless rates (1 Mbps, 2 Mbps, 5.5 Mbps, 11 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, and 54 Mbps). In addition to B and G speeds, the Cisco RV110W supports N speeds. Other options are 1-2 Mbps, for use with older wireless technology, and All, when the Cisco RV110W can transmit at all wireless rates.</p> <p>The Basic Rate is not the actual rate of data transmission. If you want to specify the Cisco RV110W rate of data transmission, configure the Transmission Rate setting.</p>
<b>Transmission Rate</b>	<p>The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select <b>Auto</b> to have the Cisco RV110W automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Cisco RV110W and a wireless client. The default is Auto.</p>
<b>N Transmission Rate</b>	<p>The rate of data transmission should be set depending on the speed of your Wireless-N networking. You can select from a range of transmission speeds, or you can select <b>Auto</b> to have the Cisco RV110W automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Cisco RV110W and a wireless client. The default is Auto.</p>

<p><b>CTS Protection Mode</b></p>	<p>The Cisco RV110W will automatically use CTS (Clear-To-Send) Protection Mode when your Wireless-N and Wireless-G devices are experiencing severe problems and are not able to transmit to the Cisco RV110W in an environment with heavy 802.11b traffic.</p> <p>This function boosts the Cisco RV110W ability to catch all Wireless-N and Wireless-G transmissions but will severely decrease performance. The default is Auto.</p>
<p><b>Beacon Interval</b></p>	<p>The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the Cisco RV110W to synchronize the wireless network.</p> <p>Enter a value between 40 and 3,500 milliseconds. The default value is 100.</p>
<p><b>DTIM Interval</b></p>	<p>This value, between 1 and 255, indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages.</p> <p>When the Cisco RV110W 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 value is 1.</p>
<p><b>Fragmentation Threshold</b></p>	<p>This value specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold.</p> <p>Setting the Fragmentation Threshold too low may result in poor network performance. Only minor reduction of the default value is recommended. In most cases, it should remain at its default value of 2346.</p>

<b>RTS Threshold</b>	<p>If you encounter inconsistent data flow, enter only minor reductions. The default value of 2347 is recommended.</p> <p>If a network packet is smaller than the preset Request to Send (RTS) threshold size, the RTS/Clear to Send (CTS) mechanism will not be enabled. The Services Ready Platform sends RTS frames to a particular receiving station and negotiates the sending of a data frame.</p> <p>After receiving an RTS, the wireless station responds with a CTS frame to acknowledge the right to begin transmission.</p>
----------------------	--

**STEP 3** Click **Save**.

## Configuring 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.

To establish a WDS link, the Cisco RV110W and other remote WDS peers must be configured in the same wireless network mode, wireless channel, wireless band selection, and encryption types (None and WEP).

**NOTE** WDS is supported on one SSID only.

To configure a WDS:

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

**STEP 2** Check the **Allow wireless signal to be repeated by a repeater** box to enable WDS.

**STEP 3** To manually enter the MAC address of a repeater, click the **Manual** button, or choose **Auto** to have the router automatically detect the remote access points.

**STEP 4** (Optional) Click the **Show Site Survey** button.

The **Available Networks Table** appears listing the available wireless network access points.

- a. (Optional) Click the **Refresh** button to update the entries in the table.
- b. In the **Available Networks Table**, select up to three access points to use as repeaters.
- c. To add the MAC addresses of the selected access points to the MAC fields below the table, click **Connect**.

**STEP 5** If you clicked the **Manual** button, enter the MAC addresses of up to three access points to use as repeaters in the **MAC 1**, **MAC 2**, and **MAC 3** fields.

**STEP 6** Click **Save**.

---

## Configuring WPS

You can configure WPS on the Cisco RV110W to allow WPS-enabled devices to more easily connect to the wireless network.

To configure WPS on client devices:

---

**STEP 1** Choose **Wireless > WPS**. The Wi-Fi Protected Setup page appears

**STEP 2** From the **SSID** drop-down menu, choose the wireless network on which to enable WPS.

**STEP 3** In the **WPS** field, check **Enable** to enable WPS. To disable WPS, uncheck the box.

**STEP 4** Configure the WPS on client devices in one of the following three ways:

- WPS Method 1
- WPS Method 2
- WPS Method 3

After you configure WPS, the following information appears at the bottom of the **WPS** page: Wi-Fi Protected Setup Status, Network Name (SSID), Security, Encryption, and Passphrase.

---

---

#### WPS Method 1

Use this method if your client device has a WPS button.

- 
- STEP 1** Click or press the WPS button on the client device.
  - STEP 2** On the **WPS** page, click the **WPS** button. When WPS configuration is completed, a dialog box appears.
  - STEP 3** Click **OK**.
- 

Refer to your client device or its documentation for additional instructions on setting up your client device.

#### WPS Method 2

Use this method if the client device has a WPS PIN number.

- 
- STEP 1** On the **WPS** page, enter the PIN number in the field.
  - STEP 2** Click **Register**.
  - STEP 3** After configuration is completed, click **OK**.
- 

Refer to your client device or its documentation for further instructions on setting up your client device.

#### WPS Method 3

If the client device requires a PIN number from the router, use the number listed in item 3 on the **WPS** page.

---



# Configuring the Firewall

## Cisco RV1 10W Firewall Features

You can secure your network by creating and applying rules that the Cisco RV1 10W uses to selectively block and allow inbound and outbound Internet traffic. You then specify how and to what devices the rules apply. To do so, you must define the following:

- Services or traffic types (examples: web browsing, VoIP, other standard services and also custom services that you define) that the router should allow or block.
- Direction for the traffic by specifying the source and destination of traffic; this is done by specifying the “From Zone” (LAN/WAN/DMZ) and “To Zone” (LAN/WAN/DMZ).
- Schedules as to when the router should apply rules.
- Keywords (in a domain name or on a URL of a web page) that the router should allow or block.
- Rules for allowing or blocking inbound and outbound Internet traffic for specified services on specified schedules.
- MAC addresses of devices whose inbound access to your network the router should block.
- Port triggers that signal the router to allow or block access to specified services as defined by port number.
- Reports and alerts that you want the router to send to you.

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



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

If you want to allow incoming traffic, you must make the router's WAN port IP address known to the public. This is called “exposing your host.” How you make your address known depends on how the WAN ports are configured; for the Cisco RV110W, you may use the IP address if a static address is assigned to the WAN port, or if your WAN address is dynamic, a DDNS (Dynamic DNS) name can be used.

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

## Configuring Basic Firewall Settings

To configure basic firewall settings:

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

**STEP 2** Configure the following firewall settings:

<b>Firewall</b>	Check <b>Enable</b> to configure firewall settings.
<b>DoS Protection</b>	Check <b>Enable</b> to enable Denial of Service protection.
<b>Block WAN Request</b>	Blocks ping requests to the Cisco RV110W from the WAN.
<b>Web Access</b>	Choose the type of web access that can be used to connect to the firewall: HTTP or HTTPS (secure HTTP).

<p><b>Remote Management Remote Access Remote Upgrade Allowed Remote IP Address Remote Management Port</b></p>	<p>See <a href="#">Configuring Remote Management</a>.</p>
<p><b>IPv4 Multicast Passthrough (IGMP Proxy)</b></p>	<p>Check <b>Enable</b> to enable multicast passthrough for IPv4.</p>
<p><b>IPv6 Multicast Passthrough (IGMP Proxy)</b></p>	<p>Check <b>Enable</b> to enable multicast passthrough for IPv6.</p>
<p><b>UPnP Allow Users to Configure Allow Users to Disable Internet Access</b></p>	<p>See <a href="#">Configuring Universal Plug and Play</a>.</p>
<p><b>Block Java</b></p>	<p>Check to block Java applets. 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.</p> <p>Enabling this setting blocks Java applets from being downloaded. Click <b>Auto</b> to automatically block Java, or click <b>Manual</b> and enter a specific port on which to block Java.</p>

<p><b>Block Cookies</b></p>	<p>Check to block cookies. Cookies are used to store session information by websites that usually require login. However, several websites use cookies to store tracking information and browsing habits. Enabling this option filters out cookies from being created by a website.</p> <p>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.</p> <p>Click <b>Auto</b> to automatically block cookies, or click <b>Manual</b> and enter a specific port on which to block cookies.</p>
<p><b>Block ActiveX</b></p>	<p>Check to block ActiveX content. 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.</p> <p>Enabling this setting blocks ActiveX applets from being downloaded.</p> <p>Click <b>Auto</b> to automatically block ActiveX, or click <b>Manual</b> and enter a specific port on which to block ActiveX.</p>
<p><b>Block Proxy</b></p>	<p>Check to block proxy servers. A proxy server (or proxy) allows computers to route connections to other computers through the proxy, thus circumventing certain firewall rules.</p> <p>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.</p> <p>Click <b>Auto</b> to automatically block proxy servers, or click <b>Manual</b> and enter a specific port on which to block proxy servers.</p>

**STEP 3** Click **Save**.

## Configuring Remote Management

You can enable remote management so you can access the Cisco RV110W from a remote WAN network.

To configure remote management, configure these settings on the **Basic Settings** page:

<b>Remote Management</b>	Check <b>Enable</b> to enable remote management.
<b>Remote Access</b>	Choose the type of web access that can be used to connect to the firewall: HTTP or HTTPS (secure HTTP).
<b>Remote Upgrade</b>	To allow remote upgrades of the Cisco RV110W, check <b>Enable</b> .
<b>Allowed Remote IP Address</b>	Click the <b>Any IP Address</b> button to allow remote management from any IP address, or enter a specific IP address in the address field.
<b>Remote Management Port</b>	Enter the port on which remote access is allowed. The default port is 443. When remotely accessing the router, you must enter the remote management port as part of the IP address. For example:  <code>https://&lt;remote-ip&gt;:&lt;remote-port&gt;</code> , or <code>https://168.10.111:443</code>



**CAUTION** When remote management is enabled, the router is accessible to anyone who knows its IP address. Because a malicious WAN user can reconfigure the Cisco RV110W and misuse it, it is highly recommended that you change the administrator and any guest passwords before continuing.

## Configuring Universal Plug and Play

Universal Plug and Play (UPnP) allows automatic discovery of devices that can communicate with the Cisco RV110W.

To configure UPnP, configure these settings on the **Basic Settings** page:

<b>UPnP</b>	Check <b>Enable</b> to enable UPnP.
<b>Allow Users to Configure</b>	Check this box to allow UPnP port-mapping rules to be set by users who have UPnP support enabled on their computers or other UPnP enabled devices. If disabled, the Cisco RV110W does not allow application to add the forwarding rule.
<b>Allow Users to Disable Internet Access</b>	Check this box to allow users to disable Internet access.

## Managing Firewall Schedules

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

### Adding or Editing a Firewall Schedule

To create or edit a schedule:

- STEP 1** Choose **Firewall > Schedule Management**.
- STEP 2** Click **Add Row**.
- STEP 3** In the **Name** field, enter a unique name to identify the schedule. This name is available on the Firewall Rule Configuration page in the **Select Schedule** list. (See [Configuring Access Rules](#).)
- STEP 4** Under **Scheduled Days**, select whether you want the schedule to apply to all days or specific days. If you choose **Specific Days**, check the box next to the days you want to include in the schedule.
- STEP 5** Under **Scheduled Time of Day**, select the time of day that you want the schedule to apply. You can either choose **All Times**, or choose **Specific Time**. If you choose **Specific Time**, enter the start and end times.

---

**STEP 6** Click **Save**.

---

## Configuring Services Management

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.

The **Services Management** page allows you to create custom services against which firewall rules can be defined. Once defined, the new service appears in the List of **Available Custom Services** table.

To create a custom service:

---

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

**STEP 2** Click **Add Row**.

**STEP 3** In the **Service Name** field, enter the service name for identification and management purposes.

**STEP 4** In the **Protocol** field, choose the Layer 4 protocol that the service uses from the drop-down menu:

- **TCP**
- **UDP**
- **TCP & UDP**
- **ICMP**

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

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

**STEP 7** Click **Save**.

---

To edit an entry, select the entry and click **Edit**. Make your changes, then click **Save**.

---

## Configuring Access Rules

### Configuring the Default Outbound Policy

The **Access Rules** page allows you to configure the default outbound policy for the traffic that is directed from the secure network (LAN) to the non-secure network (dedicated WAN/optional).

The default inbound policy for traffic flowing from the non-secure zone to the secure zone is always blocked and cannot be changed.

To configure the default outbound policy:

---

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

**STEP 2** Choose **Allow** or **Deny**.

**Note:** Ensure that IPv6 support is enabled on the Cisco RV110W to configure an IPv6 firewall. See [Configuring IPv6](#).

**STEP 3** Click **Save**.

---

### Reordering Access Rules

The order in which access rules are displayed in the access rules table indicates the order in which the rules are applied. You may want to reorder the table to have certain rules applied before other rules. For example, you may want to apply a rule allowing certain types of traffic before blocking other types of traffic.

To reorder access rules:

---

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

**STEP 2** Click **Reorder**.

**STEP 3** Check the box in the row of the rule that you want to move up or down and click the up or down arrow to move the rule up or down one line, or select the desired position of the rule in the drop-down list and click **Move to**.

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

---

## Adding Access Rules

All configured firewall rules on the Cisco RV110W are displayed in the **Access Rules Table**. This list also indicates whether the rule is enabled (active) and gives a summary of the “from/to” zone as well as the services and users the rule affects.

To create an access rule:

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

**STEP 2** Click **Add Row**.

**STEP 3** In the **Connection Type** field, choose the source of originating traffic:

- **Outbound (LAN > WAN)**—Choose this option to create an outbound rule.
- **Inbound (WAN > LAN)**—Choose this option to create an inbound rule.
- **Inbound (WAN > DMZ)**—Choose this option to create an inbound rule.

**STEP 4** From the **Action** drop-down menu, 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.
- **Allow by schedule, otherwise block**—Allows the selected type of traffic according to a schedule.

**STEP 5** From the **Services** drop-down menu, choose the service to allow or block for this rule. Choose **All Traffic** to allow the rule to apply to all applications and services, or choose a single application to block:

- Domain Name System (DNS), UDP or TCP
- File Transfer Protocol (FTP)
- Hypertext Transfer Protocol (HTTP)
- Secure Hypertext Transfer Protocol (HTTPS)
- Trivial File Transfer Protocol (TFTP)
- Internet Message Access Protocol (IMAP)
- Network News Transport Protocol (NNTP)



- Post Office Protocol (POP3)
- Simple Network Management Protocol (SNMP)
- Simple Mail Transfer Protocol (SMTP)
- Telnet
- STRMWORKS
- Terminal Access Controller Access-Control System (TACACS)
- Telnet (command)
- Telnet Secondary
- Telnet SSL
- Voice (SIP)

**STEP 6** (Optional) Click **Configure Services** to go to the **Service Management** page to configure the services before applying access rules to them.

See [Configuring Services Management](#) for more information.

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

- **Any**—The rule applies to traffic originating on any host in the local network.
- **Single Address**—The rule applies to traffic originating on a single IP address in the local network. Enter the address in the **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 8** In the **Log** field, specify whether the packets for this rule should be logged.

To log details for all packets that match this rule, choose **Always** from the drop-down menu. For example, if an outbound rule for a schedule is selected as **Block Always**, for every packet that tries to make an outbound connection for that service, a message with the packet's source address and destination address (and other information) is recorded in the log.

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

Choose **Never** to disable logging.

Note: When traffic is going from the LAN or DMZ to the WAN, the system requires rewriting the source or destination IP address of incoming IP packets as they pass through the firewall.

**STEP 9** In the **QoS Priority** field, assign a priority to IP packets of this service. The priorities are defined by QoS Level: (**1 (lowest), 2, 3, 4 (highest)**).

**STEP 10** In the **Rule Status** field, check the box to enable the new access rule.

**STEP 11** Click **Save**.

---

## Creating an Internet Access Policy

The Cisco RV110W supports several options for blocking Internet access. You can block all Internet traffic, block Internet traffic to certain PCs or endpoints, or 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.

### Adding or Editing an Internet Access Policy

To create a Internet access policy:

---

**STEP 1** Choose **Firewall > Internet Access Policy**.

**STEP 2** Click **Add Row**.

**STEP 3** In the **Status** field, check **Enable**.

**STEP 4** Enter a policy name for identification and management purposes.

**STEP 5** From the **Action** drop-down menu, choose the type of access restriction you need:

- **Always block**—Always block Internet traffic. This blocks Internet traffic to and from all endpoints. If you want to block all traffic but allow certain endpoints to receive Internet traffic, see Step 7.
- **Always allow**—Always allow Internet traffic. You can refine this to block specified endpoints from Internet traffic; see Step 7. You can also allow all Internet traffic except for certain websites; see Step 8.
- **Block by schedule**—Blocks Internet traffic according to a schedule (for example, if you wanted to block Internet traffic during the weekday business hours, but allow it after hours and on weekends).
- **Allow by schedule**—Allows Internet traffic according to a schedule.

If you chose **Block by schedule** or **Allow by schedule**, click **Configure Schedules** to create a schedule. See [Managing Firewall Schedules](#).

**STEP 6** Choose a schedule from the drop-down menu.

**STEP 7** (Optional) Apply the access policy to specific PCs to allow or block traffic coming from specific devices:

- a. In the **Apply Access Policy to the Following PCs** table, click **Add Row**.
- b. From the **Type** drop-down menu, choose how to identify the PC (by MAC address, by IP address, or by providing a range of IP addresses).
- c. In the **Value** field, depending on what you chose in the previous step, enter the one of the following:
  - MAC address (xx:xx:xx:xx:xx:xx) of the PC to which the policy applies.
  - The IP address of the of the PC to which the policy applies.
  - The starting and ending IP addresses of the range of addresses to block (for example, 192.168.1.2-192.168.1.253).

**STEP 8** To block traffic from specific websites:

- a. In the **Website Blocking** table, click **Add Row**.
- b. From the **Type** drop-down menu, choose how to block a website (by specifying the URL or by specifying a keyword that appears in the URL).
- c. In the **Value** field, enter the URL or keyword used to block the website.

For example, to block the example.com URL, choose **URL Address** from the drop-down menu and enter **example.com** in the **Value** field. To block a URL that has the keyword “example” in the URL, choose **Keyword** from the drop-down menu and enter **example** in the **Value** field.

**STEP 9** 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. Common services are available or you can define a custom service and associated ports to forward.

The **Single Port Forwarding Rules** and **Port Range Forwarding Rules** pages list all the available port forwarding rules for this device and allow you to configure port forwarding rules.

**NOTE** Port forwarding 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 forwarding rule by defining the type of traffic (TCP or UDP) and the range of incoming and outgoing ports to open when enabled.

### Configuring Single Port Forwarding

To add a single port forwarding rule:

- STEP 1** Choose **Firewall > Single Port Forwarding**. A pre-existing list of applications is displayed.
- STEP 2** In the **Application** field, enter the name of the application for which to configure port forwarding.

- 
- STEP 3** In the **External Port** field, enter the port number that triggers this rule when a connection request from outgoing traffic is made.
  - STEP 4** In the **Internal Port** field, enter the port number used by the remote system to respond to the request it receives.
  - STEP 5** From the **Protocol** drop-down menu, choose a protocol (**TCP**, **UDP**, or **TCP & UDP**).
  - STEP 6** In the **IP Address** field, enter the IP address of the host on the LAN side to which the specific IP traffic will be forwarded. For example, you can forward http traffic to port 80 of the IP address of a web server on the LAN side.
  - STEP 7** In the **Enable** field, check the **Enable** box to enable the rule.
  - STEP 8** Click **Save**.
- 

## Configuring Port Range Forwarding

To add a port range forwarding rule:

- 
- STEP 1** Choose **Firewall > Port Range Forwarding**.
  - STEP 2** In the **Application** field, enter the name of the application for which to configure port forwarding.
  - STEP 3** In the **External Port** field, specify the port number that will trigger this rule when a connection request from outgoing traffic is made.
  - STEP 4** In the **Start** field, specify the port number that begins the range of ports to forward.
  - STEP 5** In the **End** field, specify the port number that ends the range of ports to forward.
  - STEP 6** From the **Protocol** drop-down menu, choose a protocol (**TCP**, **UDP**, or **TCP & UDP**).
  - STEP 7** In the **IP Address** field, enter the IP address of the host on the LAN side to which the specific IP traffic will be forwarded.
  - STEP 8** In the **Enable** field, check the **Enable** box to enable the rule.
  - STEP 9** Click **Save**.
-

## Configuring Port Range Triggering

Port triggering allows devices on the LAN or DMZ to request one or more ports to be forwarded to them. Port triggering waits for an outbound request from the LAN/DMZ on one of the defined outgoing ports, and then opens an incoming port for that specified type of traffic.

Port triggering is a form of dynamic port forwarding while an application is transmitting data over the opened outgoing or incoming ports. Port triggering opens an incoming port for a specific type of traffic on a defined outgoing port. Port triggering is more flexible than static port forwarding (available when configuring firewall rules) because a rule does not have to reference a specific LAN IP or IP range. Ports are also not left open when not in use, thereby providing a level of security that port forwarding does not offer.

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

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

To add a port triggering rule:

- 
- STEP 1** Choose **Firewall > Port Range Triggering**.
  - STEP 2** In the **Application** field, enter the name of the application for which to configure port forwarding.
  - STEP 3** In the **Triggered Range** fields, enter 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, enter the same port number in both fields.
  - STEP 4** In the **Forwarded Range** fields, enter 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 both fields.
  - STEP 5** In the **Enable** field, check the **Enable** box to enable the rule.

---

**STEP 6** Click **Save**.

---

# Configuring VPN

## VPN Tunnel Types

A VPN provides a secure communication channel (“tunnel”) between two gateway routers or a remote worker and a gateway router. You can create different types of VPN tunnels, depending on the needs of your business. Several scenarios are described below. Read these descriptions to understand the options and the steps required to set up your VPN.

### Remote access using PPTP

In this scenario, a remote user with a Microsoft computer connects to a PPTP server at your site to access network resources. Use this option to simplify VPN setup. You do not have to configure VPN policies. Remote users can connect by using the PPTP client from a Microsoft computer. There is no need to install a VPN client. However, be aware that security vulnerabilities have been found in this protocol.

Enter the PPTP server settings and add the users on the *VPN > VPN Clients* page, in the VPN Client Setting Table. Choose **PPTP** as the user protocol. See [Creating and Managing PPTP Users](#).

### Remote Access with Cisco QuickVPN

For quick setup with basic VPN security settings, distribute Cisco QuickVPN software to your users, who can then securely access your network resources. Use this option if you want to simplify the VPN setup process. You do not have to configure VPN policies. Remote users can connect securely with the Cisco QuickVPN client and an Internet connection.

1. Add the users on the *VPN > VPN Clients* page, in the VPN Client Setting Table. Choose **QuickVPN** as the user protocol. See [Importing VPN Client Settings](#).
2. Instruct users to obtain the free Cisco QuickVPN software from Cisco.com, and install it on their computers.

To enable access via Cisco QuickVPN on this router, you must enable remote management to open port 443 for SSL. See [Configuring Basic Firewall Settings](#).



### Site-to-Site VPN

The Cisco RV110W supports Site-to-Site VPN for a single gateway-to-gateway VPN tunnel. For example, you can configure the Cisco RV110W at a branch site to connect to the router at the corporate site, so that the branch site can securely access the corporate network. The site-to-site VPN is configured in the **VPN > Basic VPN Setup** page.

## VPN Clients

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 to establish an IPsec VPN tunnel. Refer to the client software guide for detailed instructions on setup as well as the router online help.

### Configuring PPTP

Point to Point Tunneling Protocol (PPTP) is a network protocol that enables the secure transfer of data from a remote client to a business network by creating a secure VPN connection across public networks, such as the Internet.

**NOTE** When enabling the VPN on the Cisco RV110W, the LAN subnet on the Cisco RV110W is automatically changed to avoid IP address conflicts between the remote network and the local network.

To configure the PPTP VPN service:

**STEP 1** Choose **VPN > VPN Clients**.

**STEP 2** Do the following:

<b>PPTP Server</b>	Check to enable the PPTP server.
<b>IP Address for PPTP Server</b>	Enter the IP address of the PPTP server.

<b>IP Address for PPTP Clients</b>	Enter the IP address range of PPTP clients.
<b>MPPE Encryption</b>	Check the <b>Enable</b> box to enable MPPE encryption. Microsoft Point-to-Point Encryption (MPPE) is used when users set up and use a PPTP VPN client to connect to the Cisco RV110W.

**STEP 3** Click **Save**.

## Configuring NetBIOS Over VPN

To enable NetBIOS over VPN:

**STEP 1** In the **NetBIOS over VPN** field, check the box to allow NetBIOS broadcasts to travel over the VPN tunnel. By default, the NetBIOS feature is available to client policies.

**STEP 2** Click **Save**.

## Creating and Managing PPTP Users

To create PPTP users:

**STEP 1** In the **VPN Client Setting Table**, click **Add Row**.

**STEP 2** Enter this information:

<b>Enable</b>	Check to enable the user.
<b>Username</b>	Enter the username of the PPTP user (4 to 32 characters).
<b>Password</b>	Enter the password (4 to 32 characters).
<b>Protocol</b>	Choose <b>PPTP</b> from the drop-down menu.

**STEP 3** Click **Save**.

To edit the settings of a PPTP user, check its box and click **Edit**. When you are done, click **Save**.

To delete a PPTP user, check its box and click **Delete**.

## Creating and Managing QuickVPN Users

To create QuickVPN users:

**STEP 1** In the **VPN Client Setting Table**, click **Add Row**.

**STEP 2** Enter this information:

<b>Enable</b>	Check to enable the user.
<b>Username</b>	Enter the username of the QuickVPN user (4 to 32 characters).
<b>Password</b>	Enter the password (4 to 32 characters).
<b>Allow User to Change Password</b>	Check to allow the user to change the password.
<b>Protocol</b>	Choose <b>QuickVPN</b> from the drop-down menu.

**STEP 3** Click **Save**.

To edit the settings of a QuickVPN user, check its box and click **Edit**. When you are done making changes, click **Save**.

---

To delete a QuickVPN user, check its box and click **Delete**. Then, click **Save**.

## Importing VPN Client Settings

You can import VPN client setting files that contain the username and passwords of clients in a Comma Separated Value (CSV) text file.

You can use a program such as Microsoft Excel to create a CSV file containing the VPN client settings. The file should contain one row for the headings and one or more rows for the VPN clients.

For example, the following specifies the settings of two users (a PPTP user and a QuickVPN user) to import:

PROTOCOL	USERNAME	PASSWORD
PPTP	pptp-user-1	12345678
QuickVPN	qv-user-1	12345678



---

**CAUTION** Importing VPN client settings deletes existing settings.

---

To import VPN client settings:

- 
- STEP 1** Click **Browse** to locate the file.
  - STEP 2** Click **Import** to load the file.
  - STEP 3** When prompted, to delete existing VPN user settings and import the settings in the CSV file, click **Yes**.
-

## Configuring Basic VPN Settings (Site-to-Site VPN)

The Cisco RV110W supports Site-to-Site VPN for a single gateway-to-gateway VPN tunnel. In this configuration, the Cisco RV110W creates a secure connection to another VPN-enabled router. For example, you can configure the Cisco RV110W at a branch site to connect to the router at the corporate site, so that the branch site can securely access the corporate network. You could have a router like the Cisco RV220W that supports ten site-to-site VPN tunnels and have an Cisco RV110W at each remote site to provide secure connectivity.

To configure basic VPN settings for a site-to-site connection:

- 
- STEP 1** Choose **VPN > Basic VPN Setup**.
- STEP 2** In the *Connection Name* field, enter a name for the VPN tunnel.
- STEP 3** In the *Pre-Shared Key* field, enter the pre-shared key, or password, that will be exchanged between the two routers. It must be between 8 and 49 characters.
- STEP 4** In the *Endpoint Information* fields, enter the following information:
- **Remote Endpoint**—Choose the way the remote endpoint, or the router to which the Cisco RV110W will connect, is identified (by IP address - for example, *192.168.1.1* - or fully-qualified domain name - for example, *cisco.com*).
  - **Remote WAN (Internet) IP Address**—Enter the public IP address or domain name of the remote endpoint.
  - **Local WAN (Internet) IP Address**—Enter the public IP address or domain name of the local endpoint (Cisco RV110W).
- STEP 5** In the *Secure Connection Remote Accessibility* fields, enter the following information:
- **Remote LAN (Local Network) IP Address**—Enter the private network (LAN) address of the remote endpoint. This is the IP address of the internal network at the remote site.
  - **Remote LAN Subnet Mask**—Enter the private network (LAN) subnet mask of the remote endpoint.
  - **Local LAN (Local Network) IP Address**—Enter the private network (LAN) address of the local network. This is the IP address of the internal network on the Cisco RV110W.

- **Local LAN (Local Network) Subnet Mask**—Enter the private network (LAN) subnet mask of the local network (Cisco RV110W).

**Note:** The remote WAN and remote LAN IP addresses cannot exist on the same subnet. For example, a remote LAN IP address of 192.168.1.100 and a local LAN IP address of 192.168.1.115 would cause conflict when traffic is routed over the VPN. The third octet must be different so that the IP addresses are on different subnets. For example, a remote LAN IP address of 192.168.1.100 and a local LAN IP address of 192.168.2.100 is acceptable.

**STEP 6** Click **Save**.

---

## Viewing Default Values

The default values used in the basic VPN settings are those proposed by the VPN consortium and they assume you are using a pre-shared key, or password, that is known to both the Cisco RV110W and the router on the other end (for example, a Cisco RV220W). To view the default values:

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

**STEP 2** Click **View Default Settings** to view the default values.

---

For more information on these values, see [Configuring Advanced VPN Parameters](#).

---

## 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 RV110W initiates and receives VPN connections with other endpoints.

### Managing 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 manage IKE policies:

- 
- STEP 1** Choose **VPN > IPsec > Advanced VPN Setup**.
- STEP 2** In the **IKE Policy Table**, checking the box in the VPN connection row allows you to perform the following tasks:
- **Edit**—Edit properties of the IKE policy. See [Adding or Editing IKE Policies](#).
  - **Delete**—Delete the policy. (**Note:** You cannot delete an IKE policy if it is being used in a VPN policy. You must first disable and delete the VPN policy in the **VPN Policy** table.)
  - **Add Row**—Add an IKE policy. See [Adding or Editing IKE Policies](#). (**Note:** If you have a VPN connection already configured, you cannot add another without deleting the existing VPN connection.)
- STEP 3** Click **Save**.
- 

### Managing VPN Policies

To manage VPN policies:

- 
- STEP 1** Choose **VPN > IPsec > Advanced VPN Setup**.
- STEP 2** In the **VPN Policy Table**, checking the box in the VPN connection row allows you to perform the following tasks:
- **Edit**—Edit properties of the VPN policy. See [Adding or Editing VPN Policies](#).

- **Enable**—Enable the policy.
- **Disable**—Disable the policy.
- **Delete**—Delete the policy.
- **Add Row**—Add a VPN policy. See [Adding or Editing VPN Policies](#). (**Note:** If you have a VPN connection already configured, you cannot add another without deleting the existing VPN connection.)

**STEP 3** Click **Save**.

---

### Adding or Editing IKE Policies

When adding or editing IKE policies, configure the following settings:

- **Policy Name**—Enter a unique name for the policy for identification and management purposes.
- **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.



In the *IKE SA Parameters* section, the Security Association (SA) parameters define the strength and mode for negotiating the SA. You can configure the following settings:

- **Encryption Algorithm**—Choose the algorithm used to negotiate the SA:
  - **DES**
  - **3DES**
  - **AES-128**
  - **AES-192**
  - **AES-256**
- **Authentication Algorithm**—Specify the authentication algorithm for the VPN header:
  - **MD5**
  - **SHA-1**
  - **SHA2-256**

Ensure that the authentication algorithm is configured identically on both sides of the VPN tunnel (for example, the Cisco RV110W and the router to which it is connecting).

- **Pre-Shared Key**—Enter the key in the space provided. Note that the double-quote character (") is not supported in the pre-shared key.
- **Diffie-Hellman (DH) Group**—Specify the DH Group algorithm, which is used when exchanging keys. The DH Group sets the strength of the algorithm in bits. Ensure that the DH Group is configured identically on both sides of the IKE policy.
- **SA Lifetime**—Enter the interval, in seconds, after which the Security Association becomes invalid.
- **Dead Peer Detection**—Check the **Enable** box to enable this feature, or uncheck the box to disable it. Dead Peer Detection (DPD) 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. If you enable this feature, also enter these settings:
  - **DPD Delay**—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.

- **DPD Timeout**—Enter the maximum time that the Cisco RV110W should wait to receive a response to the DPD message before considering the peer to be dead.

### Adding or Editing VPN Policies

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.

When adding or editing a VPN policy, you can configure the following settings:

- **Policy Name**—Enter a unique name to identify the policy.
- **Policy Type**—Choose one of the following options:
  - **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.
- **Remote Endpoint**—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). Then enter the identifier in the space provided.

In the *Local Traffic Selection* and *Remote Traffic Section*, enter these settings:

- **Local/Remote IP**—Select the type of identifier that you want to provide for the endpoint:
  - **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. Then enter the IP address in the **Start Address** field.
  - **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. Enter the subnet's network IP address in the **Start Address** field. Enter the subnet mask, such as 255.255.255.0,

in the **Subnet Mask** field. The field automatically displays a default subnet address based on the IP address.

**IMPORTANT:** 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

For a **Manual** policy type, enter the settings in the **Manual Policy Parameters** section:

- **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:
  - DES
  - 3DES
  - AES-128
  - AES-192
  - AES-256
- **Key-In**—Enter the encryption key of the inbound policy. The length of the key depends on the encryption algorithm chosen:
  - DES—8 characters
  - 3DES—24 characters
  - AES-128—16 characters
  - AES-192—24 characters
  - AES-256—32 characters
- **Key-Out**—Enter the encryption key of the outbound policy. The length of the key depends on the encryption algorithm chosen, as shown above.

- **Integrity Algorithm**—Select the algorithm used to verify the integrity of the data:
  - MD5
  - SHA-1
  - SHA2-256
- **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
- **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.

For an **Auto** policy type, enter the settings in the **Auto Policy Parameters** section.

- **SA-Lifetime**—Enter the duration of the Security Association 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.
- **Encryption Algorithm**—Select the algorithm used to encrypt the data.
- **Integrity Algorithm**—Select the algorithm used to verify the integrity of the data.
- **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.
- **Select IKE Policy**—Choose the IKE policy that will define the characteristics of phase 1 of the negotiation. Click **View** to view or edit the existing IKE policy that is configured on the Cisco RV110W.

---

## Configuring Certificate Management

The Cisco RV110W uses digital certificates for IPsec VPN authentication and SSL validation (for HTTPS). You can generate and sign your own certificates using functionality available on the Cisco RV110W.

### Generating a New Certificate

You can generate a new certificate to replace the existing certificate on the Cisco RV110W.

To generate a certificate:

- 
- STEP 1** Choose **VPN > Certificate Management..**
  - STEP 2** Click the **Generate a New Certificate** button.
  - STEP 3** Click **Generate Certificate.**
- 

### Importing Certificates

You can import certificate previously saved to a file using **Export for Admin** button.

To import a certificate:

- 
- STEP 1** Choose **VPN > Certificate Management..**
  - STEP 2** Click the **Import Certificate From a File** button.
  - STEP 3** Click **Browse** and locate the certificate file.
  - STEP 4** Click **Install Certificate.**
-

---

#### Exporting Certificates for Admin

The certificate for administrator contains the private key and should be stored in a safe place as a backup. If the Cisco RV110W configuration is reset to the factory default settings, this certificate can be imported and restored on the router.

To export a certificate for Admin:

---

**STEP 1** Choose **VPN > Certificate Management..**

**STEP 2** Click **Export for Admin.**

On a PC, the Device Manager saves the admin.pem file in the C:\Documents and Settings\userid\My Documents\Downloads.

---

#### Exporting Certificates for Client

The certificate for client allows QuickVPN users to securely connect to the Cisco RV110W. QuickVPN users must place the certificate in the install directory of the QuickVPN client.

To export a certificate for client:

---

**STEP 1** Choose **VPN > Certificate Management..**

**STEP 2** Click **Export for Client.**

On a PC, the Device Manager saves the client.pem file in the C:\Documents and Settings\userid\My Documents\Downloads.

---

## Configuring VPN Passthrough

VPN passthrough allows VPN traffic that originates from VPN clients to pass through the Cisco RV110W.

To configure VPN passthrough:

---

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

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

---

<b>IPsec</b>	Check <b>Enable</b> to allow IP security tunnels to pass through the Cisco RV110W.
<b>PPTP</b>	Check <b>Enable</b> to allow PPTP tunnels to pass through the Cisco RV110W.
<b>L2TP</b>	Check <b>Enable</b> to allow Layer 2 Tunneling Protocol (L2TP) tunnels to pass through the Cisco RV110W.

**STEP 3** Click **Save**.

---

# Configuring Quality of Service (QoS)

## Configuring Bandwidth Management

You can use the Cisco RV110W bandwidth management feature to manage the bandwidth of the traffic flowing from the secure network (LAN) to the insecure network (WAN).

### Configuring Bandwidth

You can limit the bandwidth to reduce the rate at which the Cisco RV110W transmits data. You can also use a bandwidth profile to limit the outbound traffic, thus preventing the LAN users from consuming all of the bandwidth of the Internet link.

To set the upstream and downstream bandwidth:

- 
- STEP 1** Choose **QoS > Bandwidth Management**.
  - STEP 2** In the **Bandwidth Management** field, check **Enable**. The maximum bandwidth provided by your ISP appears in the **Bandwidth** section.



**STEP 3** In the **Bandwidth Table**, enter the following information for the WAN interface:

<b>Upstream</b>	The bandwidth (kb/s) used for sending data to the Internet.
<b>Downstream</b>	The bandwidth (kb/s) used for receiving data from the Internet.

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

### Configuring Bandwidth Priority

In the **Bandwidth Priority Table**, you can assign priorities to services to manage bandwidth usage.

To configure bandwidth priority:

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

**STEP 2** In the **Bandwidth Management** field, check **Enable**. The maximum bandwidth provided by your ISP appears in the **Bandwidth** section.

**STEP 3** In the **Bandwidth Priority Table**, click **Add Row**.

**STEP 4** Enter this information:

<b>Enable</b>	Check to enable bandwidth management for this service.
<b>Service</b>	Choose the service to prioritize.
<b>Direction</b>	Choose the direction of the traffic you want to prioritize ( <b>downstream</b> or <b>upstream</b> ).
<b>Priority</b>	Choose the priority of the service ( <b>low</b> , <b>normal</b> , <b>medium</b> , or <b>high</b> ).

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

To edit the settings of an entry in the table, check the relevant box and click **Edit**. When you are done making changes, click **Save**.

To delete an entry from the table, check the relevant box and click **Delete**. Then, click **Save**.

To add a new service definition, click the **Service Management** button. You can define a new service to use for all firewall and QoS definitions. See [Configuring Services Management](#).

## Configuring QoS Port-Based Settings

You can configure QoS settings for every LAN port on the Cisco RV110W. The Cisco RV110W supports 4 priority queues that allow for traffic prioritization per physical switch port.

To configure QoS settings for the Cisco RV110W LAN ports:

**STEP 1** Choose **QoS > QoS Port-Based Settings**.

**STEP 2** For each port in the **QoS Port-Based Settings Table**, enter this information:

<p><b>Trust Mode</b></p>	<p>Choose one of the following options from the drop-down menu:</p> <ul style="list-style-type: none"> <li>▪ <b>Port</b>—This setting enables the port based on QoS. You can then set the traffic priority for a particular port. The traffic queue priority starts at the lowest priority of 1 and ends with the highest priority of 4.</li> <li>▪ <b>DSCP</b>—Differentiated Services Code Point (DSCP). Enabling this feature prioritizes the network traffic across the LAN based on the DSCP queue mapping on the <b>DSCP Settings</b> page.</li> <li>▪ <b>CoS</b>—Class of Service (CoS).</li> </ul>
<p><b>Default Traffic Forwarding Queue for Untrusted Devices</b></p>	<p>Choose a priority level for outbound traffic (1 to 4).</p>

**STEP 3** Click **Save**.

---

To restore the default port-based QoS settings, click **Restore Default**. Then, click **Save**.

## Configuring CoS Settings

You can map CoS priority settings to the traffic forwarding queue on the Cisco RV110W.

You can use the link to the QoS Port-Based Settings Page to map the CoS priority setting to the QoS queue.

To map CoS priority settings to the traffic forwarding queue:

---

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

**STEP 2** For each CoS priority level in the **CoS Settings 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 3** Click **Save**.

---

To restore the default port-based QoS settings, click **Restore Default**. Then, click **Save**.

## Configuring DSCP Settings

You can use the **DSCP Settings** page to configure DSCP-to-QoS queue mapping.

To configure DSCP-to-QoS queue mapping:

---

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

**STEP 2** Choose whether to only list RFC values or to list all DSCP values in the **DSCP Settings Table** by clicking the relevant button.

**STEP 3** For each DSCP value in the **DSCP Settings Table**, choose a priority level from the **Queue** drop-down menu.

---

This maps the DSCP value to the selected QoS queue.

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

---

To restore the default DSCP settings, click **Restore Default**. Then, click **Save**.

# Administering Your Cisco RV110W

## Setting Password Complexity

The Cisco RV110W can enforce minimum password complexity requirement for password changes.

To configure password complexity settings:

- 
- STEP 1** Choose **Administration > Password Strength**.
- STEP 2** In the *Password Complexity Settings* field, check **Enable**.
- STEP 3** Configure password complexity settings:

<b>Minimum Password Length</b>	Enter the minimum password length (0-64 characters).
<b>Minimum number of character classes</b>	<p>Enter a number representing one of the following character classes:</p> <ul style="list-style-type: none"> <li>▪ Uppercase letters.</li> <li>▪ Lowercase letters.</li> <li>▪ Numbers.</li> <li>▪ Special characters available on a standard keyboard.</li> </ul> <p>By default, passwords must contains characters from at least three of these classes.</p>
<b>The new password must be different than the current one</b>	Check <b>Enable</b> to require that new passwords differ from the current password.

<b>Password Aging</b>	Check <b>Enable</b> to expire passwords after a specified time.
<b>Password aging time</b>	Enter the number of days after which the password expires (1–365). The default is 180 days.

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

## Configuring User Accounts

Your device supports two user accounts for administering and viewing settings: a read-write access administrative user (default user name and password: cisco) and a read-only access guest user (default user name and password: guest).

You can set and change the username and password for both the administrator and guest accounts.

**NOTE** By default, the guest user account is inactive. It is highly recommended to change the username and password while activating the account.

To configure the user accounts:

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

**STEP 2** In the *Account Activation* field, check the boxes for the accounts you want to activate. (The admin account must be active.)

**STEP 3** (Optional) To edit the administrator account, under *Administrator Account Setting*, check **Edit Administrator Settings**. To edit the guest account, under *Guest Settings*, check **Edit Guest Settings**. Enter the following information:

<b>New Username</b>	Enter a new username.
<b>Old Password</b>	Enter the current password.

<b>New Password</b>	Enter the new password. We recommended that you make sure that the password contains no dictionary words from any language, and is a mix of letters (both uppercase and lowercase), numbers, and symbols. The password can be up to 64 characters long.
<b>Retype New Password</b>	Re-enter the new password.

- STEP 4** To import user names and passwords from a CSV file:
- In the **Import User Name & Password** field, click **Browse**.
  - Locate the file and click **Open**.
  - Click **Import**.
- STEP 5** Enter the old password.
- 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. You can configure timeout for the Admin and Guest accounts.

To configure session timeout:

- STEP 1** Choose **Administration > Session Timeout**.
- STEP 2** In the **Administrator Inactivity Timeout** field, enter the number, in minutes, before a session times out due to inactivity. Choose **never** to allow the administrator to stay logged in permanently.
- STEP 3** In the **Guest Inactivity Timeout** field, enter the number, in minutes, before a session times out due to inactivity. Choose **never** to allow the administrator to stay logged in permanently.
- STEP 4** Click **Save**.

## Configuring Simple Network Management (SNMP)

Simple Network Management Protocol (SNMP) lets you monitor and manage your router from an SNMP manager. SNMP provides a remote means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

### Configuring SNMP System Information

In the **SNMP System Information** section of the **SNMP** page, you can enable SNMP.

Before you can use SNMP, install SNMP software on your computer. The Cisco RV110W supports only SNMPv3 for SNMP management. The Cisco RV110W supports SNMPv1/2/3 for SNMP trap messages.

To enable SNMP:

- 
- STEP 1** Choose **Administration > SNMP**.
  - STEP 2** Check **Enable** to enable SNMP.
  - STEP 3** Enter this information:

<b>SysContact</b>	Enter the name of the contact person for this firewall (for example, <b>admin</b> or <b>John Doe</b> .)
<b>SysLocation</b>	Enter the physical location of the firewall (for example, <b>Rack #2, 4th Floor</b> .)
<b>SysName</b>	Enter a name for easy identification of the firewall.

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

### Editing SNMPv3 Users

You can configure SNMPv3 parameters for the two default Cisco RV110W user accounts (Admin and Guest).

To configure SNMPv3 settings:

- 
- STEP 1** Choose **Administration > SNMP**.
  - STEP 2** Under **SNMPv3 User Configuration**, configure the following settings:



<b>UserName</b>	Select the account to configure ( <b>admin</b> or <b>guest</b> ).
<b>Access Privilege</b>	Displays the access privileges of the selected user account.
<b>Security Level</b>	Choose the SNMPv3 security level:  <b>No Authentication and No Privilege</b> —Doesn't require any Authentication and Privacy.  <b>Authentication and No Privilege</b> —Submit only Authentication algorithm and password.  <b>Authentication and Privilege</b> —Submit Authentication/privacy algorithm and password.
<b>Authentication Algorithm Server</b>	Select the type of authentication algorithm ( <b>MD5</b> or <b>SHA</b> ).
<b>Authentication Password</b>	Enter the authentication password.
<b>Privacy Algorithm</b>	Choose the type of privacy algorithm ( <b>DES</b> or <b>AES</b> ).
<b>Privacy Password</b>	Enter the privacy password.

**STEP 3** Click **Save**.

### Configuring the SNMP Traps

The fields in the **SNMP Trap Configuration** section allow you to configure an SNMP agent to which the firewall sends trap messages (notifications).

To configure the traps:

**STEP 1** Choose **Administration > SNMP**.

**STEP 2** Under **Trap Configuration**, configure the following settings:

<b>IP Address</b>	Enter the IP address of the SNMP manager or trap agent.
<b>Port</b>	Enter the SNMP trap port of the IP address to which the trap messages will be sent.

<b>Community</b>	Enter the community string to which the agent belongs.  Most agents are configured to listen for traps in the Public community.
<b>SNMP Version</b>	Select the SNMP version: <b>v1</b> , <b>v2c</b> , or <b>v3</b> .

**STEP 3** Click **Save**.

## Using Diagnostic Tools

The Cisco RV110W provides several diagnostic tools to help you troubleshoot network problems.

- **Network Tools**
- **Configuring Port Mirroring**

### Network Tools

Use network tools to troubleshoot the network.

#### Using PING

You can use the PING utility to test connectivity between this router and another device in the network. You can also use the Ping tool to test connectivity to the Internet by pinging a fully qualified domain name (for example, [www.cisco.com](http://www.cisco.com)).

To use PING:

- STEP 1** Choose **Administration > Diagnostics > Network Tools**.
- STEP 2** In the **IP Address / Domain Name** field, enter the device IP address or a fully qualified domain name such as [www.cisco.com](http://www.cisco.com) to ping.
- STEP 3** Click **Ping**. The ping results appear. These results tell you whether the device is reachable.
- STEP 4** Click **Close** when done.

---

### Using Traceroute

The Traceroute utility displays all the routers present between the destination IP address and this router. The router displays up to 30 hops (intermediate routers) between this router and the destination.

To use Traceroute:

- 
- STEP 1** Choose **Administration > Diagnostics > Network Tools**.
  - STEP 2** In the **IP Address / Domain Name** field, enter the IP address to trace.
  - STEP 3** Click **Traceroute**. The Traceroute results appear.
  - STEP 4** Click **Close** when done.
- 

### Performing a DNS Lookup

You can use the Lookup tool to find out the IP address of host (for example, a Web, FTP, or Mail server) on the Internet.

To retrieve the IP address of a Web, FTP, Mail or any other server on the Internet, type the Internet Name in the text box and click **Lookup**. If the host or domain entry exists, you will see a response with the IP address. A message stating “Unknown Host” indicates that the specified Internet Name does not exist.

To use the Lookup tool:

- 
- STEP 1** Choose **Administration > Diagnostics > Network Tools**.
  - STEP 2** In the **Internet Name** field, enter the Internet name of the host.
  - STEP 3** Click **Lookup**. The nslookup results appear.
  - STEP 4** Click **Close** when done.
-

---

## Configuring Port Mirroring

Port mirroring monitors network traffic by sending copies of all incoming and outgoing packets from one port to a monitoring port. You can use port mirroring as a diagnostic or debugging tool, especially when fending off an attack or viewing user traffic from LAN to WAN to see if users are accessing information or websites they are not supposed to.

The LAN host (PC) should use a static IP address to avoid any issues with port mirroring. DHCP leases can expire for a LAN host and can cause port mirroring to fail so if a static IP address is not configured for the LAN host.

To configure port mirroring:

- 
- STEP 1** Choose **Administration > Diagnostics > Port Mirroring**.
  - STEP 2** In the **Mirror Source** field, select the ports to mirror.
  - STEP 3** From the **Mirror Port** drop-down menu, choose a mirror port. If you use a port for mirroring, do not use it for any other traffic.
  - STEP 4** Click **Save**.
- 

## Configuring Logging

The Cisco RV110W allows you to configure logging options.

### Configuring Logging Settings

To configure logging:

- 
- STEP 1** Choose **Administration > Logging > Log Settings**.
  - STEP 2** In the **Log Mode** field, check **Enable**.
  - STEP 3** Click **Add Row**.

**STEP 4** Configure the following settings:

<b>Remote Log Server</b>	Enter the IP address of the log server that will collect logs.
<b>Log Severity for Local Log and Email</b>	<p>Click to choose the severity of logs you want to configure. Note that all log types above a selected log type are automatically included and you cannot deselect them. For example, choosing “error” logs automatically includes emergency, alert, and critical logs in addition to error logs.</p> <p>The event severity levels are listed from the highest severity to the lowest severity, as follows:</p> <ul style="list-style-type: none"> <li>▪ <b>Emergency</b>—System is not usable.</li> <li>▪ <b>Alert</b>—Action is needed.</li> <li>▪ <b>Critical</b>—System is in a critical condition.</li> <li>▪ <b>Error</b>—System is in error condition.</li> <li>▪ <b>Warning</b>—System warning occurred.</li> <li>▪ <b>Notification</b>—System is functioning properly, but a system notice occurred.</li> <li>▪ <b>Information</b>—Device information.</li> <li>▪ <b>Debugging</b>—Provides detailed information about an event. Choosing this severity uses large amounts of logs to be generated and is not recommended during normal router operation.</li> </ul>
<b>Enable</b>	To enable these logging settings, check this box.

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

To edit an entry in the **Logging Setting Table**, select the entry and click **Edit**. Make your changes, then click **Save**.

## Configuring the E-Mailing of Logs

You can configure the Cisco RV110W to send logs by email. We recommend that you set up a separate email account for sending and receiving logs.

You must first set up the severity of logs you want to capture; see [Configuring Logging Settings](#).

To configure the e-mailing of logs:

- STEP 1** Choose **Administration > Logging > E-mail Settings**.
- STEP 2** To enable the e-mailing of log events, check **Enable**.
- STEP 3** The minimum email log severity of logs you want to capture appears. To change this, click **Configure Severity**.
- STEP 4** Configure the following settings:

<b>E-mail Server Address</b>	Enter the address of the SMTP server. This is the mail server associated with the email account you've setup (for example, <i>mail.companyname.com</i> ).
<b>E-mail Server Port</b>	Enter the SMTP server port. If your email provider requires a special port for email, enter it here. Otherwise, use the default (25).
<b>Return E-mail Address</b>	Enter the return email address that the Cisco RV110W will send messages to if logs from the router to the send-to email address are undeliverable.
<b>Send to E-mail Address (1)</b>	Enter an email address to which to send logs (for example, <i>logging@companyname.com</i> ).
<b>Send to E-mail Address (2) (Optional)</b>	Enter an additional email address to which to send logs.
<b>Send to E-mail Address (3) (Optional)</b>	Enter an additional email address to which to send logs.
<b>E-mail Encryption (SSL)</b>	To enable email encryption, check <b>Enable</b> .

<b>Authentication with SMTP Server</b>	If the SMTP (mail) server requires authentication before accepting connections, choose the type of authentication from the drop-down menu: <b>None</b> , <b>LOGIN</b> , <b>PLAIN</b> , and <b>CRAM-MD5</b> .
<b>E-mail Authentication Username</b>	Enter the email authentication username (example, <i>logging@companyname.com</i> ).
<b>E-mail Authentication Password</b>	Enter the email authentication password (for example, the password used to access the email account you have set up to which to send logs).
<b>E-mail Authentication Test</b>	Click <b>Test</b> to test email authentication.

**STEP 5** In the **Send E-Mail Logs by Schedule** section, configure the following settings:

<b>Unit</b>	Choose the unit of time for the logs ( <b>Never</b> , <b>Hourly</b> , <b>Daily</b> , or <b>Weekly</b> ). If you choose <b>Never</b> , logs are not sent.
<b>Day</b>	If you chose a weekly schedule for sending logs, choose the day of the week on which to send the logs.
<b>Time</b>	If you chose a daily or weekly schedule for sending logs, choose the time of day at which to send the logs.

**STEP 6** Click **Save**.

---

## Configuring Bonjour

Bonjour is a service advertisement and discovery protocol. On the Cisco RV110W, Bonjour only advertises the default services configured on the device when Bonjour is enabled.

To enable Bonjour:

- 
- STEP 1** Choose **Administration > Bonjour**.
  - STEP 2** Check **Enable** to enable Bonjour.
  - STEP 3** To enable Bonjour for a VLAN listed in the **Bonjour Interface Control Table**, check the corresponding **Enable Bonjour** box.

You can enable Bonjour on specific VLANs. Enabling Bonjour on a VLAN allows devices present on the VLAN to discover Bonjour services available on the router (such as http/https).

For example, if a VLAN is configured with an ID of 2, devices and hosts present on VLAN 2 cannot discover Bonjour services running on the router unless Bonjour is enabled for VLAN 2.

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

## Configuring Date and Time Settings

You can configure your time zone, whether or not to adjust for Daylight Savings Time, and with which Network Time Protocol (NTP) server to synchronize the date and time. The router then gets its date and time information from the NTP server.

To configure NTP and time settings:

- 
- STEP 1** Choose **Administration > Time Settings**. The current time is displayed.



**STEP 2** Configure this information:

<b>Time Zone</b>	Select your time zone, relative to Greenwich Mean Time (GMT).
<b>Adjust for Daylight Savings Time</b>	If supported for your region, check the <b>Adjust for Daylight Savings Time</b> box.  This check box is enabled if you click <b>Auto</b> in the <b>Set Date and Time</b> field below.
<b>Daylight Saving Mode</b>	Choose either <b>By date</b> (you enter the specific date on which daylight saving mode starts) or <b>Recurring</b> (you enter the month, week, day of week, and time on which daylight saving time starts). Enter the appropriate information in the “from” and “to” fields.
<b>Daylight Saving Offset</b>	Choose the offset from Coordinated Universal Time (UTC) from the drop-down menu.
<b>Set Date and Time</b>	Select how to set the date and time.
<b>NTP Server</b>	To use the default NTP servers, click the <b>Use Default</b> button.  To use a specific NTP server, click the <b>User Defined NTP Server</b> and enter the fully-qualified domain name or IP address of the NTP servers in the two available fields.
<b>Enter Date and Time</b>	Enter the date and time.

**STEP 3** 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 firewall 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 firewall settings from this file.



**CAUTION** During a restore operation, do not try to go online, turn off the firewall, shut down the PC, or use the firewall until the operation is complete. This should take about a minute. When the test light turns off, wait a few more seconds before using the firewall.

### Backing Up the Configuration Settings

To backup or restore the configuration:

**STEP 1** Choose **Administration > Backup/Restore Settings**.

**STEP 2** Select the configuration to back up or to clear:

<b>Startup configuration</b>	<p>Select this option to download the startup configuration. The Startup Configuration is the most current running configuration that the Cisco RV110W uses.</p> <p>If the router startup configuration has been lost, use this page to copy the Backup Configuration to the Startup configuration and have all of their previous configuration information intact.</p> <p>You can download the Startup Configuration to other Cisco RV110Ws for easy deployment.</p>
<b>Mirror configuration</b>	<p>Select this option to instruct the Cisco RV110W to back up the Startup Configuration after 24 hours of operation without any change in the startup configuration.</p>
<b>Backup configuration</b>	<p>Select this option to back up the current configuration settings.</p>

**STEP 3** To download a backup file based on the selected configuration option, click **Download**.

By default, the file (startup.cfg, mirror.cfg, or backup.cfg) is downloaded in the default Downloads folder; for example, *C:\Documents and Settings\admin\My Documents\Downloads\*.

**STEP 4** To clear the selected configuration, click **Clear**.

---

### Restoring the Configuration Settings

You can restore a previously-saved configuration file:

---

**STEP 1** Choose **Administration > Backup/Restore Settings**.

**STEP 2** In the Configuration Upload field, select the configuration to upload (**Startup Configuration** or **Backup Configuration**).

**STEP 3** Click **Browse** to locate the file.

**STEP 4** Select the file and click **Open**.

**STEP 5** Click **Start to Upload**.

The Cisco RV110W uploads the configuration file and uses the settings it contains to update the Startup Configuration. Then the Cisco RV110W restarts and uses the new configuration.

---

### Copying the Configuration Settings

You copy the Startup Configuration to the Backup Configuration to ensure you have a backup copy in case you forget your username and password and get locked out of the Device Manager. In this case, the only way to get back into the Device Manager is to reset the Cisco RV110W to factory default.

The Backup Configuration file remains in memory and allows the backed up configuration information to be copied to the Startup Configuration, which restores all of the settings.

To copy a configuration (for example, to copy a startup configuration to the backup configuration):

---

**STEP 1** Choose **Administration > Backup/Restore Settings**.

**STEP 2** In the **Copy** field, choose the source and destination configurations from the drop-down menus.

---

**STEP 3** Click **Start to Copy**.

---

### Generating an Encryption Key

The router allows you to generate an encryption key to protect the backup files.

To generate an encryption key:

---

**STEP 1** Choose **Administration > Backup/Restore Settings**.

**STEP 2** Click **Show Advanced Settings**.

**STEP 3** In the box, enter the seed phrase used to generate the key.

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

---

## Upgrading Firmware or Change the Language

You can upgrade to a newer version of the firmware or change the language of the router by using the **Administration > Firmware/Language Upgrade** page.



**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 memory is being written to may corrupt it and render the router unusable.

---

### Upgrading the Firmware

To update the router with a newer version of the firmware:

---

**STEP 1** Choose **Administration > Firmware/Language Upgrade**.

**STEP 2** (Optional) Click **Download** to download the latest version of the firmware.

**STEP 3** In the **File Type** field, click the **Firmware Image** button.

**STEP 4** Click **Browse** to locate and select the downloaded firmware.

---

- 
- STEP 5** (Optional) To reset the Cisco RV110W to default factory settings after the firmware is upgraded, check **Reset all configurations/settings to factory defaults**.



**CAUTION** Resetting the Cisco RV110W to default factory settings erases all of your custom settings.

---

- STEP 6** Click **Start 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.

- STEP 7** Choose **Status > System Summary** to make sure the router installed the new firmware version.
- 

### Changing the Language

To change the language:

---

- STEP 1** Choose **Administration > Firmware/Language Upgrade**.
- STEP 2** In the **File Type** field, click the **Language File** button.
- STEP 3** Click **Browse** to locate and select the language file.
- STEP 4** Click **Start Upgrade**.
- 

## Restarting the Cisco RV110W

To restart the router:

---

- STEP 1** Choose **Administration > Reboot**.
- STEP 2** 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 use 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 using the router.

---

To restore factory defaults to the router:

- 
- STEP 1** Choose **Administration > Restore Factory Defaults**.
  - STEP 2** Click **Default**.
- 

## Running the Setup Wizard

To run the Setup Wizard:

- 
- STEP 1** Choose **Administration > Setup Wizard**.
  - STEP 2** Follow the online instructions.
-







# Viewing the Cisco RV110W Status

## Viewing the Dashboard

The **Dashboard** page provides you with a bird's-eye view of important router information.

To view the Dashboard:

- 
- STEP 1** Choose **Status > Dashboard**.
  - STEP 2** To display an interactive view of the router 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 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

- **System Name**—The name of the device.
- **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](#).

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

### LAN (Local Network) Interface

- **MAC Address**—The MAC address of the router.
- **IPv4 Address**—The local IP address of the router.
- **IPv6 Address**—The local IP address of the router (if IPv6 is enabled).
- **DHCP Server**—The status of the router IPv4 DHCP server (enabled or disabled).
- **DHCPv6 Server**—The status of the router IPv6 DHCP server (enabled or disabled).

To view the LAN settings, click **details**. For more information, see [Configuring the LAN Settings](#).

### WAN (Internet) Information

- **IPv4 Address**—The IP address of the router WAN port.
- **IPv6 Address**—The IP address of the router WAN port, if IPv6 is enabled.
- **State**—The state of the Internet connection (up or down).

To view the WAN settings, click **details**. For more information see [Configuring the WAN Settings](#).

#### Wireless Networks

Lists the status of the four wireless network SSIDs.

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

#### VPN

- **QuickVPN Users**—The number of QuickVPN users.
- **PPTP Users**—The number of Point-to-Point Tunneling Protocol (PPTP) users.

## Viewing the System Summary

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

To view a summary of system settings:

- STEP 1** Choose **Status > System Summary**.
- STEP 2** Click **Refresh** to obtain the latest information.

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

#### System Information

- **Firmware Version**—Current software version the device is running.
- **Firmware MD5 Checksum**—The message-digest algorithm used to verify the integrity of files.
- **Locale**—The language installed on the router.
- **Language Version**—The version of the installed language pack. The language pack version should be compatible with the currently- installed firmware. In some cases, an older language pack may be used with a newer firmware image. The router will check the language pack version to see if it is compatible with the current firmware version.
- **Language MD5 Checksum**—The MD5 checksum of the language pack.
- **CPU Model**—Chipset of CPU currently used.

- **Serial Number**—Serial number of the device.
- **System Up Time**—How long the system has been running.
- **Current Time**—Time of day.
- **PID VID**—Product ID and version ID of the device.

#### IPv4 Configuration

- **LAN IP**—LAN address of the device.
- **WAN IP**—WAN Address of the device. You can release the current IP address and obtain a new one by clicking **Release** or **Renew**.
- **Gateway**—The IP address of the gateway to which the Cisco RV110W is connected (for example, the cable modem).
- **Mode**—Displays **Gateway** if NAT is enabled, or **Router**.
- **DNS 1**—Primary DNS server IP address of the WAN port.
- **DNS 2**—Secondary DNS server IP address of the WAN port.
- **DDNS**—Indicates whether the Dynamic DNS is enabled or disabled.

#### IPv6 Configuration

- **LAN IP**—The LAN address of the device.
- **WAN IP**—The WAN Address of the device.
- **Gateway**—The IP address of the gateway to which the Cisco RV110W is connected (for example, the cable modem).
- **NTP**—Network Time Protocol server (hostname or IPv6 address).
- **Prefix Delegation**—The IPv6 prefix returned from the device at the ISP that is given to IP addresses on the Cisco RV110W.
- **DNS 1**—The IP address of the primary DNS server.
- **DNS 2**—The IP address of the secondary DNS server.

#### Wireless Summary

- **SSID 1**—The public name of the first wireless network.
  - **Security**—The security setting for SSID 1.
- **SSID 2**—The public name of the second wireless network.

- **Security**—The security setting for SSID 2.
- **SSID 3**—The public name of the third wireless network.
  - **Security**—The security setting for SSID 3.
- **SSID 4**—The public name of the fourth wireless network.
  - **Security**—The security setting for SSID 4.

### Firewall Setting Status

- **Dos (Denial of Service)**—Whether DoS prevention is on or off.
- **Block WAN Request**—Whether WAN request blocking is on or off.
- **Remote Management**—Whether remote management is on or off (for example, if the Cisco RV110W Device Manager can be accessed remotely).

### VPN Setting Status

- **QuickVPN Connections Available**—The number of available QuickVPN connections.
- **PPTP VPN Connections Available**—The number of available PPTP VPN connections.
- **Connected QuickVPN Users**—The number of connected QuickVPN users.
- **Connected PPTP VPN Users**—The number of connected PPTP VPN users.

## 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** From the **Refresh Rate** drop-down menu, choose a refresh rate.
  - STEP 3** (Optional) By default, byte data is displayed in bytes and other numerical data is displayed in long form. To show the bytes in kilobytes (KB) and the numerical data in rounded up form, check **Show Simplified Statistic Data** and click **Save**.

**STEP 4** To reset the wireless statistics counters, click **Clear Count**.

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

<b>SSID Name</b>	The name of the wireless network.
<b>Packet</b>	The number of received/sent wireless packets reported to the radio over all configured and active SSIDs.
<b>Byte</b>	The number of received/sent bytes of information reported to the radio, over all configured SSIDs.
<b>Error</b>	The number of received/sent packet errors reported to the radio, over all configured SSIDs.
<b>Dropped</b>	The number of received/sent packets dropped by the radio, over all configured SSIDs.
<b>Multicast</b>	The number of multicast packets sent over this radio.
<b>Collisions</b>	The number of packet collisions reported to the router.

**NOTE** The counters are reset when the device is rebooted.

## Viewing the VPN Status

The **VPN** page displays the status of VPN connections.

To view VPN user connection status, choose **Status > VPN Status**.

The **VPN** page displays this information:

<b>Username</b>	The username of the VPN user associated with the QuickVPN or PPTP tunnel.
<b>Remote IP</b>	Displays the IP address of the remote QuickVPN client. This could be a NAT/Public IP if the client is behind the NAT router.
<b>Status</b>	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.
<b>Start Time</b>	The time of the VPN user establishing a connection.
<b>End Time</b>	The time of the VPN user ending a connection.
<b>Duration (Seconds)</b>	The duration between the VPN user establishing and ending a connection.
<b>Protocol</b>	The protocol the user uses, QuickVPN or PPTP.

You can change the status of a connection to either establish or disconnect the configured VPN client.

To terminate an active VPN connection, click **Disconnect**.

## Viewing the IPSec Connection Status

The IPSec Connection status shows the status of active VPN policies on the Cisco RV110W. (These policies are configured on the **VPN > Advanced VPN Setup** page.) To view the IPSec connection status:

**STEP 1** Choose **Status > IPSec Connection Status**.

**STEP 2** The table displays the following information:

- **Refresh Rate**—Choose the rate at which you want the data display to clear and display the newest data.

- **Show Simplified Statistic Data**—By default, byte data is displayed in bytes and other numerical data is displayed in long form. To show the bytes in kilobytes (KB) and the numerical data in rounded up form, check **Show Simplified Statistic Data**.
- **Policy Name**—Name of the VPN policy for which data is displayed.
- **Local or Remote**—Displays the local and remote IP addresses.
- **Start Time and End Time**—Displays the start and end times of the IPSec connections.
- **Duration**—Displays the elapsed time for which the connection is or was active.
- **Packet**—Displays the received (Rx) and transmitted (Tx) packets on the connection.
- **Byte**—Displays the received (Rx) and transmitted (Tx) bytes on the connection.
- **State**—Displays the state of the connection (for example, active or not connected).
- **Action**—Displays actions you can perform on the connection (for example, disconnect).

**STEP 3** If you made any changes, click **Save**.

---

## Viewing Logs

The **View Logs** page allows you to view the Cisco RV110W 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 filter logs, or specify the severity of logs to display, check the boxes next to the log type and click **Go**. Note that all log types above a selected log type are automatically included and you cannot deselect them. For example, choosing “error” logs automatically includes emergency, alert, and critical logs in addition to error logs.



The event severity levels are listed from the highest severity to the lowest severity, as follows:

- **Emergency**—System is not usable.
- **Alert**—Action is needed.
- **Critical**—System is in a critical condition.
- **Error**—System is in error condition.
- **Warning**—System warning occurred.
- **Notification**—System is functioning properly, but a system notice occurred.
- **Informational**—Device information.
- **Debugging**—Provides detailed information about an event.

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

To save all log messages from the firewall to the local hard drive, click **Save Logs**.

To specify the number of entries to show per page, choose a number from the drop-down menu.

Use the page navigation buttons to move between log pages.

## Viewing Connected Devices

The **Connected Devices** page displays information about the active devices connected to the Cisco RV110W.

The IPv4 ARP Table displays information from devices that have responded to the Cisco RV110W address resolution protocol (ARP) request. If a device does not respond to the request, it is removed from the list.

The IPv6 NDP Table displays all IPv6 neighbor discover protocol (NDP) devices connected to the Cisco RV110W local link.

To view connected devices:

- STEP 1** Choose **Status > Connected Devices**.
- STEP 2** In the *IPv4 ARP Table*, you can specify the types of interfaces to display by selecting an option from the **Filter** drop-down menu. You can choose one of the following options:

<b>All</b>	Displays a list of all devices connected to the router.
<b>Wireless</b>	Displays a list of all devices connected through the wireless interface.
<b>Wired</b>	Displays a list of all devices connected through the Ethernet ports on the router.
<b>WDS</b>	Displays a list of all Wireless Distribution System (WDS) device connected to the router.

## Viewing Port Statistics

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

To view port statistics:

- STEP 1** Choose **Status > Port Statistics**.
- STEP 2** From the **Refresh Rate** drop-down menu, choose a refresh rate. This causes the page to re-read the statistics from the router and refresh the page.
- STEP 3** (Optional) By default, byte data is displayed in bytes and other numerical data is displayed in long form. To show the bytes in kilobytes (KB) and the numerical data in rounded up form, check **Show Simplified Statistic Data** and click **Save**.
- STEP 4** To reset the port statistics counters, click **Clear Count**.

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

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

<b>Interface</b>	The name of the network interface.
<b>Packet</b>	The number of received/sent packets.
<b>Byte</b>	The number of received/sent bytes of information per second.
<b>Error</b>	The number of received/sent packet errors.
<b>Dropped</b>	The number of received/sent packets that were dropped.
<b>Multicast</b>	The number of multicast packets sent over this radio.
<b>Collisions</b>	The number of signal collisions that occurred on this port. A collision occurs when the port tries to send data at the same time as a port on another router or computer that is connected to this port.

## Viewing the GuestNet Status

The guest network statistics displays information about the wireless guest network configured on the Cisco RV110W. To view the guest network status, choose **Status > GuestNet Status**. The following information is displayed:

- **Host Name**—Device connected to the guest network.
- **IP Address**—IP address assigned to the connected device.
- **MAC Address**—MAC or hardware address of the connected device.
- **Time Left**—Remaining time that the device can be connected to the guest network. (Time limits are configured in the **Wireless > Basic Settings > Guest Net Settings** page.)
- **Action**—Actions you can perform on the connected device (for example, disconnect).

## Viewing the Cisco RV110W Status

Viewing the GuestNet Status

8

---

# Using Cisco QuickVPN

## Overview

This appendix explains how to install and use the Cisco QuickVPN software that can be downloaded from [Cisco.com](https://www.cisco.com). QuickVPN works with computers running Windows 7, Windows XP, Windows Vista, or Windows 2000. (Computers using other operating systems will have to use third-party VPN software.)

This appendix includes the following sections:

- [Before You Begin](#)
- [Installing the Cisco QuickVPN Software](#)
- [Using the Cisco QuickVPN Software](#)

## 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 Basic Firewall Settings](#).
- STEP 2** Create Quick VPN user accounts. See [Configuring PPTP](#). After a user account is created, the credentials can be used by the Quick VPN client.
-

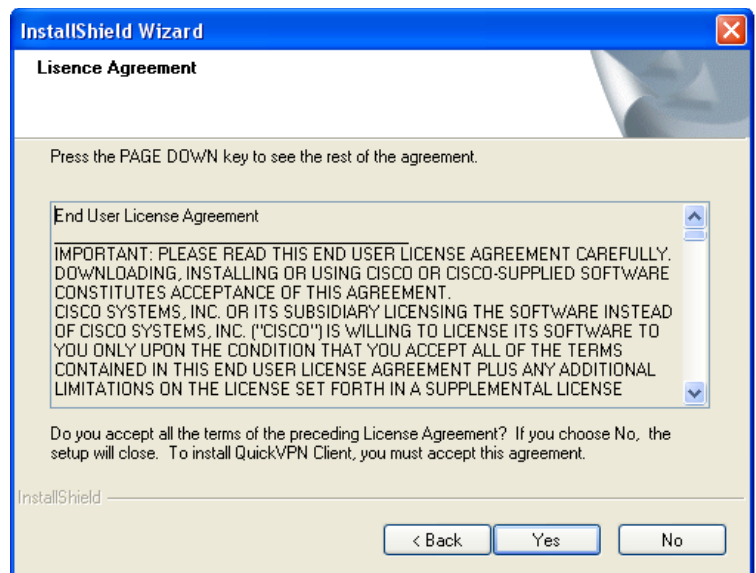
## Installing the Cisco QuickVPN Software

### Installing from the CD-ROM

- STEP 1** Insert the Cisco RV110W CD-ROM into your CD-ROM drive. After the Setup Wizard begins, click the **Install QuickVPN** link.

The License Agreement window appears.

#### License Agreement

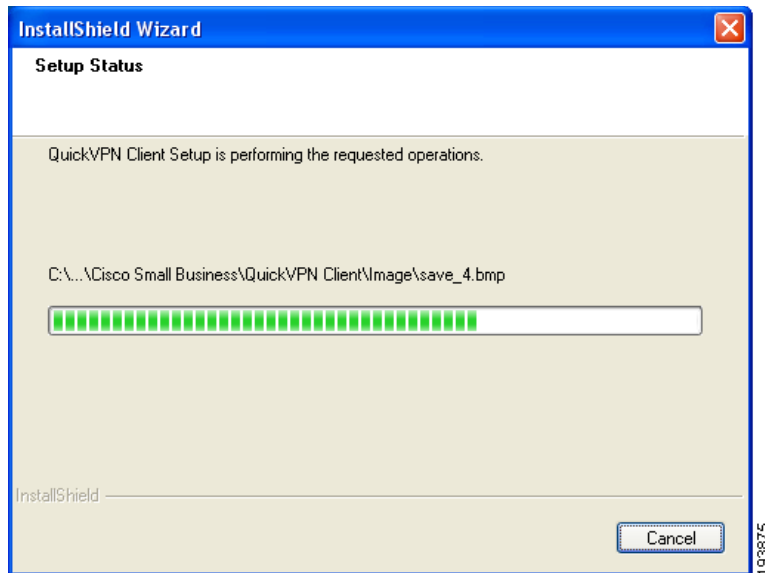


- STEP 2** Click **Yes** to accept the agreement.
- STEP 3** Click **Browse** and choose where to copy the files to (for example, C:\Cisco\QuickVPN Client).

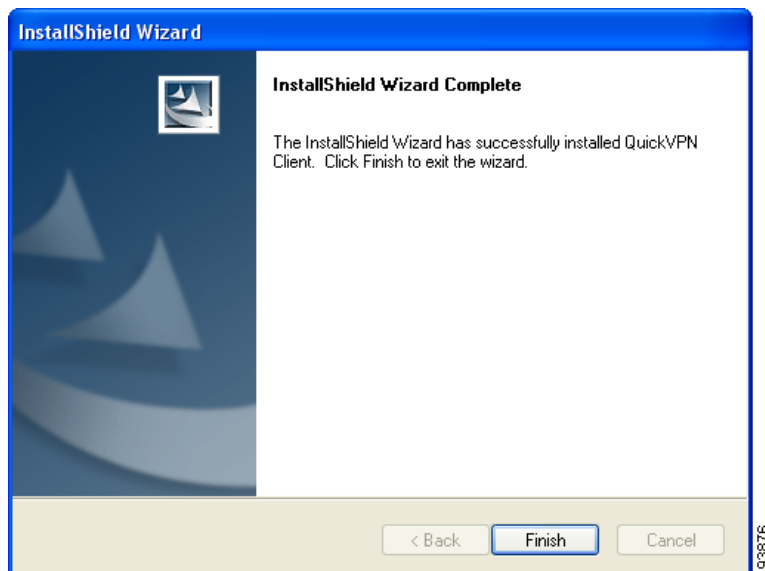
### STEP 4 Click **Next**.

The Setup Wizard copies the files to the chosen location.

### Copying Files



### Finished Installing Files



### STEP 5 Click **Finish** to complete the installation. Proceed to **Downloading and Installing from the Internet**.

---

### Downloading and Installing from the Internet

---

- STEP 1** In **Where to Go From Here** go to the Software Downloads link.
  - STEP 2** Enter Cisco RV1 10W 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 icon on your desktop or in the system tray.



QuickVPN Desktop Icon



QuickVPN Tray Icon—  
No Connection

The QuickVPN Login window appears.

- STEP 2** In the **Profile Name** field, enter a name for your profile.
- STEP 3** In the **User Name** and **Password** fields, enter the User Name and Password that were created in **Creating and Managing QuickVPN Users**.
- STEP 4** In the **Server Address** field, enter the IP address or domain name of the Cisco RV1 10W.
- STEP 5** In the **Port For QuickVPN** field, enter the port number that the QuickVPN client uses to communicate with the remote VPN router, or keep the default setting, **Auto**.
- STEP 6** To save this profile, click **Save**.  
To delete this profile, click **Delete**. For information, click **Help**.



**NOTE** If there are multiple sites to which you need to create a tunnel, you can create multiple profiles, but only one tunnel can be active at a time.

**STEP 7** To begin your QuickVPN connection, click **Connect**.

The connection progress displays: *Connecting, Provisioning, Activating Policy, and Verifying Network*.

**STEP 8** After 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.

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

**STEP 9** If you clicked **Change Password** and have permission to change your own password, the **Connect Virtual Private Connection** window appears.

**STEP 10** 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.

**STEP 11** Click **OK** to save your new password.

---

**NOTE** You can change your password only if the **Allow User to Change Password** box has been checked for that username. See [Creating and Managing QuickVPN Users](#).

## Where to Go From Here

Cisco provides a wide range of resources to help you obtain the full benefits of the Cisco RV110W.

### Product Resources

Support	
Cisco Support Community	<a href="http://www.cisco.com/go/smallbizsupport">www.cisco.com/go/smallbizsupport</a>
Online Technical Support and Documentation (Login Required)	<a href="http://www.cisco.com/support">www.cisco.com/support</a>
Phone Support Contacts	<a href="http://www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html">www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html</a>
Software Downloads (Login Required)	Go to <a href="http://tools.cisco.com/support/downloads">tools.cisco.com/support/downloads</a> , and enter the model number in the Software Search box.
Product Documentation	
Cisco RV110W	<a href="http://www.cisco.com/en/US/products/ps9923/tsd_products_support_series_home.html">www.cisco.com/en/US/products/ps9923/tsd_products_support_series_home.html</a>
Cisco Partner Central (Partner Login Required)	<a href="http://www.cisco.com/web/partners/sell/smb">www.cisco.com/web/partners/sell/smb</a>
Marketplace	<a href="http://www.cisco.com/go/marketplace">www.cisco.com/go/marketplace</a>