ADMINISTRATION GUIDE

Cisco Small Business

CVR100W Wireless-N VPN Router

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**. 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)

© 2013 Cisco Systems, Inc. All rights reserved.

OL-26942-02

Contents

Chapter 1: Introduction 7

Product Overview 7
- LAN Ethernet Interface 8
- Wireless Access Point 8
- Security 8
- Firewall and VPN Access 8
- Wireless Distribution System 9
- Quality of Service 9
- Virtual Networks 9

Getting to Know the CVR100W 10
- Front Panel 10
- Back Panel 12
- Default Settings 13

Installing the CVR100W 13
- Placement Tips 13
- Wall Mounting 14

Connecting the CVR100W 14

Getting Started with the Configuration 15

Changing the Default Administrative Password 16

Using the Connection Status Page 18

Using the Getting Started Page 19
- Returning to the Connection Status Page 20
- Changing Your Preferred Language 20
- Viewing the Help Files 20

Verifying the Hardware Installation 20

Connecting to Your Wireless Network 21

Chapter 2: Viewing CVR100W Status 22

Viewing the Dashboard 22

Viewing System Summary 25

Viewing Connected Devices 27

Viewing DHCP Leased Clients 28
Viewing Port Statistics 29
Viewing Wireless Statistics 30
Viewing Guest Network Status 31
Viewing VPN Status 32
Viewing Logs 33
Viewing IPsec Connection Status 34
Viewing CSC Information 35
Viewing NETSTAT Information 36

Chapter 3: Configuring Network 38

Configuring WAN Settings 38
Configuring Automatic Configuration (DHCP) 39
Configuring PPPoE 39
Configuring Static IP 40
Configuring Optional Settings 41
Cloning the MAC Address 42
Configuring LAN Settings 43
Configuring Basic LAN Settings 43
IPv4 43
Configuring DHCP 44
Configuring VLAN 45
Configuring Static DHCP 47
Configuring a DMZ Host 48
Configuring Routing 48
Configuring Operating Mode 48
Configuring Dynamic Routing 49
Configuring Static Routing 50
Configuring Inter-VLAN Routing 51
Viewing the Routing Table 51
Configuring Dynamic DNS 52

Configuring IP Mode 53
Configuring IPv6 54
Configuring IPv6 WAN Settings 54
Setting the IP Mode 54
Configuring DHCPv6 55
Configuring a Static IP Address 55
Configuring IPv6 LAN Settings 56
Setting the IP Mode 56
Configuring IPv6 LAN Settings 56
Configuring DHCPv6 Settings 57
Configuring IPv6 Address Pools 58
Configuring IPv6 Static Routing 59
Configuring Routing (RIPng) 60
Configuring IPv6-to-IPv4 Tunneling 61
Viewing IPv6 Tunnel Status 61
Configuring Router Advertisement 61
Configuring Advertisement Prefixes 63

Chapter 4: Configuring Wireless Network 65

Wireless Security 65
Wireless Security Tips 65
General Network Security Guidelines 67
CVR100W Wireless Networks 67
Configuring Basic Wireless Settings 68
Configuring Wireless Radio Settings 68
Configuring Wireless Network Settings 69
Configuring Wireless Security 71
Configuring MAC Address Filtering 74
Configuring Time of Day Access 75
Configuring Guest Net 75
Configuring Cisco Simple Connect 76
Configuring Advanced Wireless Settings 79
Configuring WDS 82

Configuring WPS 83

Chapter 5: Configuring Firewall 85

CVR100W Firewall Features 85
Access Rules 85
Port Forwarding 87
Configuring Basic Firewall Settings 87
Managing Firewall Schedules 89
Configuring Service Management 90
Configuring Access Control 91
Default Access Control Policy 91
Configuring Access Rules 91
Configuring Internet Access Rules 94
Configuring Single Port Forwarding 95
Configuring Port Range Forwarding 96
Configuring Port Range Triggering 97

Chapter 6: Configuring VPN 98

VPN Tunnel Types 98
Remote Access with Cisco QuickVPN 98
Site-to-Site VPN 99
Configuring VPN Clients 99
Creating and Managing QuickVPN Users 99
Importing VPN Client Settings 100
Configuring Basic VPN Setup 101
Viewing Default VPN Settings 101
Configuring Basic VPN Settings 102
Configuring Advanced VPN Setup 104
Configuring Global Advanced VPN Settings 104
Managing IKE Policies 105
Configuring VPN Policies 107

Managing Certificates 111
Generating a New Certificate 111
Importing Certificates 112
Exporting Certificates for Admin 112
Exporting Certificates for Client 112
Configuring VPN Passthrough 113

Chapter 7: Configuring Quality of Service (QoS) 114

Configuring Bandwidth Management 114
Configuring Bandwidth 114
Configuring Bandwidth Priority 115
Configuring QoS Port-Based Settings 116
Configuring CoS Settings 117
Configuring DSCP Settings 117

Chapter 8: Administering Your CVR100W 119

Configuring Password Complexity 120
Configuring Administrator Account Settings 121
Configuring Remote Management 122
Configuring Port Management 123
Configuring Do-Not-Disturb Mode 124
Configuring System Time 124
Configuring Bonjour 125
Using Diagnostic Tools 126
Network Tools 126
Configuring Port Mirroring 127
Configuring Logging 128
Configuring Logging Settings 128
Configuring Remote Syslog Server 129
Backing Up and Restoring System Configuration 129
Backing Up Your Current Configuration 130

Restoring Your Configuration from a Saved Configuration File 130
Upgrading Firmware 131
Rebooting the CVR100W 132
Restoring the Factory Defaults 132
Running the Setup Wizard 133

Chapter 9: Using Cisco Simple Connect 136
About Cisco Simple Connect 136
Configuring Cisco Simple Connect 138
Connecting to CSC Wireless Network 140
Customizing Your QR Code 141

Appendix A: Using Cisco QuickVPN 143
Before You Begin 143
Installing the Cisco QuickVPN Software 144
Using the Cisco QuickVPN Software 144

Appendix B: Where to Go From Here 148

1

Introduction

This chapter provides information to familiarize you with the product features, guide you through the installation process, and get started by using web-based Configuration Utility. It includes the following sections:

- **Product Overview**
- **Getting to Know the CVR100W**
- **Installing the CVR100W**
- **Connecting the CVR100W**
- **Getting Started with the Configuration**
- **Changing the Default Administrative Password**
- **Using the Connection Status Page**
- **Using the Getting Started Page**
- **Verifying the Hardware Installation**
- **Connecting to Your Wireless Network**

Product Overview

Thank you for choosing the Cisco CVR100W Wireless-N VPN Router. The CVR100W provides simple, affordable, secure business-class connectivity to the Internet for small office/home office (SOHO) and remote professionals.

The CVR100W 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.

LAN Ethernet Interface

The CVR100W provides four full-duplex 10/100 Fast Ethernet LAN interfaces that can connect up to four devices. You can connect a Cisco Small Business switch to one of the available ports to expand your network as needed.

Wireless Access Point

The CVR100W's 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.

Security

The CVR100W implements WPA Personal, WPA Enterprise, WPA2 personal, WPA2 Enterprise, and WEP Security, along with other security features, such as SSID broadcast, MAC address filtering, and access control by schedule per SSID.

Firewall and VPN Access

The CVR100W incorporates a Stateful Packet Inspection (SPI)-based firewall with Denial of Service (DoS) protection, URL filtering, and access control by schedule to help keep business assets safe.

Up to three client-to-gateway VPN tunnels can be established by using QuickVPN to allow mobile or remote workers to securely access your corporate resources through encrypted virtual links. Users connecting through a VPN tunnel are attached to your company's network with secure access to files, e-mail, and your intranet as if they were in the building.

The CVR100W supports site-to-site VPN for a single gateway-to-gateway VPN tunnel. In this configuration, the CVR100W creates a secure connection to another VPN-enabled router. For example, you can configure the CVR100W 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 a CVR100W at each remote site to provide secure connectivity.

Wireless Distribution System

The CVR100W's wireless access point supports Wireless Distribution System (WDS), which allows the wireless coverage to be expanded without wires.

Quality of Service

The CVR100W supports Wi-Fi Multimedia (WMM) and Wi-Fi Multimedia Power Save (WMM-PS) for quality of service (QoS).

The CVR100W also supports 802.1p, Differentiated Services Code Point (DSCP), and class of service (CoS) 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.

Virtual Networks

The CVR100W 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.

Getting to Know the CVR100W

Before using the CVR100W, familiarize yourself with its buttons, lights, and interfaces found in this section.

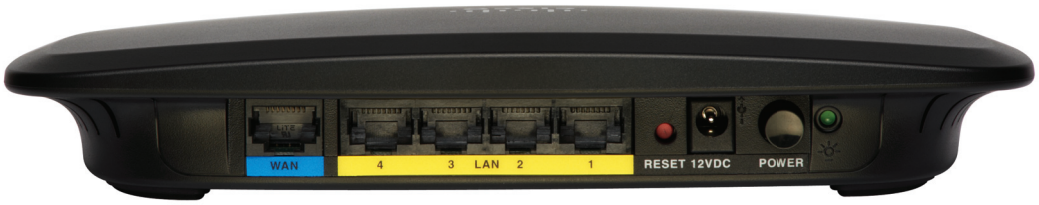
Front Panel

There are three buttons and eight lights on the front panel.

Do-Not-Disturb Mode Button	This button turns on or turns off all lights. This button does not affect the normal operation of the CVR100W. ▪ When this button is on, all lights on the front panel are off and the Do-Not-Disturb Mode light on the back panel is solid green. ▪ When this button is off, all lights on the front panel are on and the Do-Not-Disturb Mode light on the back panel is off.
WPS Button	This button configures wireless access for devices in your network that are WPS-enabled.
Wireless Button	This button enables or disables the wireless module.

LAN (1-4)	The numbered lights correspond to the LAN ports on the back panel of the CVR100W. ▪ Solid blue when the CVR100W is connected to a device through the corresponding LAN port (1, 2, 3, or 4). ▪ Flashes blue when the CVR100W is sending or receiving data over that LAN port. ▪ Off when the LAN port has no connection.
WPS	▪ Solid blue when the WPS connection is configured. ▪ Flashes blue once per second when the WPS progress is experiencing problems. ▪ Off when the WPS connection is configured or there is no WPS connection.
Wireless	▪ Solid blue when the wireless module is enabled with 100% Wi-Fi power. ▪ Solid amber when the wireless module is enabled with 50% Wi-Fi power. ▪ Flashes blue when the CVR100W is sending or receiving data on the wireless module. ▪ Off when the wireless module is disabled.
WAN	▪ Solid blue when the CVR100W is connected to the Internet through your cable or DSL modem. ▪ Flashes blue when the CVR100W is sending or receiving data through the WAN port. ▪ Off when the WAN port has no connection.
POWER	▪ Solid blue when the CVR100W is powered on and is operating normally. ▪ Flashes blue when the system is booting or the system is upgrading the firmware. ▪ Off when the CVR100W is powered off.

Back Panel



WAN	The WAN (Internet) port is connected to your Internet device, such as a cable or DSL modem.
LAN (1–4)	These ports provide the LAN connection to network devices, such as PCs, print servers, or switches.
RESET	The **RESET** button has two functions: ▪ **Reboot:** If the CVR100W has problems connecting to the Internet, press the **RESET** button for at least one second but no more than five seconds with a paper clip or a pencil tip. ▪ **Restore to Factory Defaults:** If you are experiencing extreme problems with the CVR100W and have tried all other troubleshooting measures, press and hold in the **RESET** button for more than five seconds. This reboots the unit and restores the factory defaults. The settings that you have previously made to the CVR100W are lost.
12VDC	The 12VDC port is where you connect the supplied power adapter (12V/0.5 A).
Power	Press this button to power the CVR100W on and off.
Do-Not-Disturb Mode Light	▪ Solid green when the Do-Not-Disturb Mode button is turned on and the CVR100W is operating normally. ▪ Flashes green when the Do-Not-Disturb Mode button is turned on, but the Internet connection has problems. ▪ Off when the Do-Not-Disturb Mode button is turned off.

Default Settings

These are the default settings used when configuring your CVR100W for the first time.

Parameter	Default Value
Username	cisco
Password	cisco
LAN IP	192.168.1.1
DHCP Range	192.168.1.100 to 192.168.1.149

NOTE Press and hold the **RESET** button for more than five seconds to reboot the unit and restore the factory defaults. Changes that you have previously made to the CVR100W settings are lost.

Installing the CVR100W

You can place your CVR100W on a desktop or mount it on a wall.

Placement Tips

- **Ambient Temperature**—To prevent the CVR100W 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 CVR100W.
- **Mechanical Loading**—Be sure that the CVR100W is level and stable to avoid any hazardous conditions.

Place the CVR100W horizontally on a flat surface so that it sits on its four rubber feet.

Wall Mounting

The CVR100W can be wall-mounted. The wall-mounting hardware is user-supplied. The ports on the back panel must face either upward or downward when mounting the CVR100W to a wall.

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

Connecting the CVR100W

By default, the wireless module of the CVR100W is enabled. For the initial configuration, we recommend that you connect to the CVR100W with an Ethernet cable. Of course, you can also use a wireless connection. To connect the PC to the CVR100W's wireless network for the first time, use the default SSID name and pre-shared key that are provided on the product label at the bottom of the CVR100W. See **Connecting to Your Wireless Network** for more information.

STEP 1 Power off all equipment, including the cable or DSL modem, the PC that you will use to connect to the CVR100W, and the CVR100W itself.

STEP 2 Connect the supplied power adapter to the **12VDC** port on the back panel of the CVR100W. Plug the other end of the power adapter into an electrical outlet. Make sure that the **POWER** button is turned off.

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

STEP 3 Connection one end of an Ethernet cable to your cable or DSL modem. Connect the other end to the WAN port on the back panel.

STEP 4 Connect one end of a different Ethernet cable to one of the LAN ports on the back panel. Connect the other end to an Ethernet port on the PC that you will use to run web-based Configuration Utility.

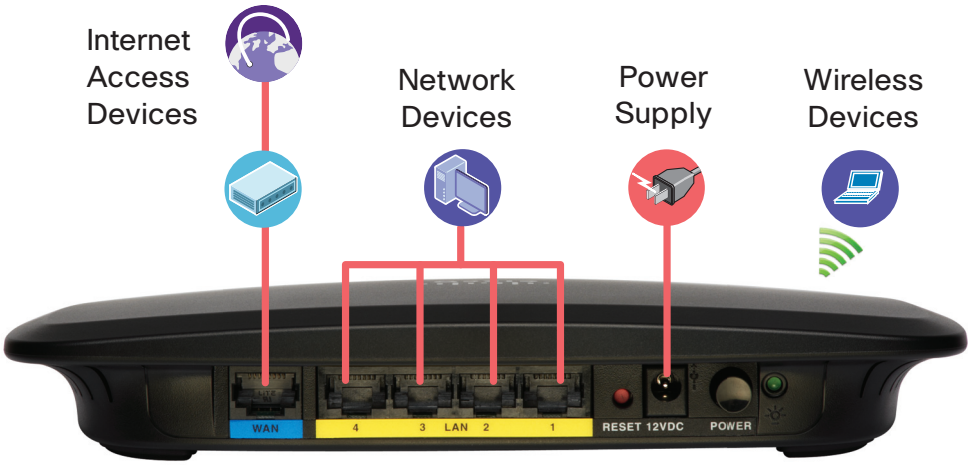
NOTE Skip this step if you want to connect the PC to the CVR100W through a wireless connection.

STEP 5 Power on all connected devices, including the cable or DSL modem and the PC, and wait until the connections are active.

STEP 6 Press the **POWER** button on the back panel to power on the CVR100W.

STEP 7 To connect the PC to your wireless network for the first time, you must configure the wireless connection using the default SSID name and pre-shared key. See **Connecting to Your Wireless Network** for more information.

A sample configuration is illustrated here.



Getting Started with the Configuration

The Setup Wizard and web-based Configuration Utility are supported on Microsoft Internet Explorer 6.0 or later, Mozilla Firefox 3.0 or later, Apple Safari 3.0 or later, and Google Chrome 5.0 or later.

To log in to web-based Configuration Utility and complete the initial configuration by using the Setup Wizard:

STEP 1 Start a computer that you connected to the CVR100W. The computer becomes a DHCP client of the CVR100W 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 CVR100W.

NOTE The CVR100W automatically changes its IP address to 10.10.10.1 when its default IP address conflicts with another device in your network.

STEP 3 When the login page appears, choose the language that you prefer to use in the utility, and then enter the username and password.

The default username is **cisco**. The default password is **cisco**. Both username and password are case sensitive.

STEP 4 Click **Log In**. The Setup Wizard will now launch.

STEP 5 Follow the on-screen prompts to complete the initial configuration. See **Running the Setup Wizard** for more information on completing the Setup Wizard configuration.

For security reasons, you must change the password from its default setting at your first login. Please write this password down for future reference. A blank password is not recommended.

Passwords should not contain dictionary words from any language or be the default password. They should contain a mixture of uppercase and lowercase letters, numbers, and symbols. Passwords must be at least 8 but no more than 64 characters in length.

After the Setup Wizard is complete, the Connection Status page appears. See **Using the Connection Status Page** for more information.

Changing the Default Administrative Password

The administrative password protects your CVR100W from unauthorized access. For security reasons, you must change the password from its default setting at your first login.

You can change the default administrative password as instructed by the Setup Wizard (see **Running the Setup Wizard**) or by following the instructions in the **Configuring Administrator Account Settings** section. If you exit the Setup Wizard without saving your settings at your first login by clicking **Exit**, the Change Password window opens.

By default, the password strength enforcement is enabled on the CVR100W. The Change Password window displays the minimum password complexity requirements as follows:

- Passwords cannot be the same as the username.
- Passwords cannot be the same as the current password.
- Passwords must be at least 8 but no more than 64 characters in length.
- Passwords must contain at least three of these character classes: uppercase letters, lowercase letters, digits, and special characters.

NOTE You can modify the minimum password complexity requirements in the **Administration** > **Password Complexity** page. See **Configuring Administrator Account Settings**.

To enter a new password in the Change Password window:

STEP 1 Enter the following information:

- **Old Password:** Enter the current password.
- **New Password:** Enter a new password.
- **Confirm Password:** Enter the new password again for confirmation.
- **Password Strength Meter:** Displays the strength of the password that you entered.
  - **Red:** Password fails to meet the minimum complexity requirements.
  - **Yellow:** Password meets the minimum requirements but the password strength is weak.
  - **Green:** Password is strong.
- **Disable Password Strength Enforcement:** Check to disable password strength enforcement (nor recommended).

STEP 2 Click **Save and Exit** to save your changes.

The Connection Status page opens. You are required to log into the utility with the new password before you do any other tasks.

Using the Connection Status Page

The Connection Status page displays the current WAN, LAN, and WLAN status of the CVR100W.

Field	Description
WAN	
Status	Shows whether the WAN port obtains an IP address successfully or not. If the WAN port is connected to the Internet, the network addressing mode that you use to connect to the Internet will be displayed.
IP	IP address of the WAN port that is accessible from the Internet.
Mask	Subnet mask for the WAN port.
Gateway	Default gateway for the WAN port.
DNS	IP addresses for the primary DNS server and the secondary DNS server.
LAN	
Host	Name of the LAN host that is connected to the CVR100W.
IP	IP address of the connected LAN host.
MAC	MAC address of the connected LAN host.
WLAN	
Wi-Fi Power	Shows whether the Wi-Fi signal strength is 100%, 50%, or off.

You can perform the following actions:

- To refresh the data on the screen, click **Refresh**.
- To log out the utility, click **Log out**.
- To launch the Setup Wizard, click **Setup Wizard**.

- To configure other advanced settings, click **Advanced Settings**. You will be first directed to the Getting Started page. See **Using the Getting Started Page** for more information.
- To learn more information about your CVR100W, click **Product Resources**.

Using the Getting Started Page

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

Initial Settings	
Change Default Administrator Password	Click this link to open the **Administration** > **User** page where you can change the administrator username and password. See **Configuring Administrator Account Settings**.
Launch Setup Wizard	Click this link to launch the Setup Wizard.
Configure WAN Settings	Click this link to open the **Networking** > **WAN** > **Internet Setup** page. See **Configuring WAN Settings**.
Configure LAN Settings	Click this link to open the **Networking** > **LAN** > **LAN Configuration** page. See **Configuring LAN Settings**.
Configure Wireless Settings	Click this link to open the **Wireless** > **Basic Settings** page. See **Configuring Basic Wireless Settings**.
Quick Access	
Upgrade Router Firmware	Click this link to open the **Administration** > **Firmware Upgrade** page. See **Upgrading Firmware**.
Add VPN Clients	Click this link to open the **VPN** > **VPN Clients** page. See **Configuring VPN Clients**.
Configure Firewall	Click this link to open the **Firewall** > **Basic Settings** page. See **Configuring Basic Firewall Settings**.

Device Status	
System Summary	Click this link to open the **Status** > **System Summary** page. See **Viewing System Summary**.
Wireless Status	Click this link to open the **Status** > **Wireless Statistics** page. See **Viewing Wireless Statistics**.
VPN Status	Click this link to open the **Status** > **VPN Status** page. See **Viewing VPN Status**.
Other Resources	
CVR100W Resources	Click this link to open the CVR100W Resources page.
Support	Click this link to visit the Cisco support community.

Returning to the Connection Status Page

To return to the Connection Status page, click the **Home Page** link near the top right corner of the page.

Changing Your Preferred Language

To change the language that you prefer to use in the web-based Configuration Utility, select the language from the **Language** drop-down menu near the top right corner of the page.

Viewing the Help Files

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

Verifying the Hardware Installation

To verify the hardware installation, complete the following tasks:

- Check the light states. They are described in **Getting to Know the CVR100W**.

- 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.
- 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 CVR100W using the Setup Wizard.

NOTE If you want to connect a device to your wireless network to do the initial configuration for the first time, use the default SSID name and pre-shared key are provided on the product label at the bottom of the CVR100W.

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.

2

Viewing CVR100W Status

This chapter describes how to view real-time statistics and other information about the CVR100W and includes the following sections:

- Viewing the Dashboard
- Viewing System Summary
- Viewing Connected Devices
- Viewing DHCP Leased Clients
- Viewing Port Statistics
- Viewing Wireless Statistics
- Viewing Guest Network Status
- Viewing VPN Status
- Viewing Logs
- Viewing IPsec Connection Status
- Viewing CSC Information
- Viewing NETSTAT Information

Viewing the Dashboard

The Dashboard page displays information about the CVR100W and its current settings.

To view the Dashboard:

STEP 1 Choose **Status** > **Dashboard**.

STEP 2 From the **Refresh Rate** drop-down menu, choose a refresh rate.

STEP 3 To display an interactive view of the back panel of the CVR100W, click **Show Panel View**.

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

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

The port's connection information includes:

Summary	
Type	Type of the port.
Interface	Shows if it is a WAN or a LAN interface.
Link Status	Shows if the port is connected or disconnected.
Speed Status	Speed and duplex settings of the port.
Auto Negotiation	Shows if the Auto Negotiation is enabled or disabled on this port.
Statistics	
TX Frames	Number of frames transmitted by the port.
RX Frames	Number of frames received by the port.

The Dashboard page displays the following information:

Device Information	
System Name	Unit name of the CVR100W.
Firmware Version	Firmware version that the CVR100W is currently using.
Serial Number	Serial number of the CVR100W.
Resource Utilization	

CPU	Current CPU utilization.
Memory	Current memory utilization.
Current Time	Time of day.
System Up Time	Duration for which the system has been running.
Do-Not-Disturb Mode	Shows if the Do-Not-Disturb mode is enabled or disabled.

Syslog Summary

Indicates whether logging is enabled for these event categories:

- Emergency
- Alert
- Critical
- Error
- Warning

To view complete logs, click **details**. See **Viewing Logs** for more information.

To configure the logging settings, click **manage logging**. See **Configuring Logging** for more information.

LAN (Local Network) Interface

To view complete LAN settings, click **details**. See **Configuring LAN Settings** for more information.

MAC Address	MAC address of the CVR100W.
IPv4 Address	Local IPv4 address of the CVR100W.
IPv6 Address	Local IPv6 address of the CVR100W (if IPv6 is enabled).
DHCP Server	Shows if the DHCP server is enabled or disabled.
DHCPv6 Server	Shows if the DHCPv6 server is enabled or disabled (if IPv6 is enabled).

WAN (Internet) Information	
To view complete WAN settings, click **details**. See **Configuring WAN Settings** for more information.	
MAC Address	MAC address of the WAN port.
IPv4 Address	IPv4 address of the WAN port.
IPv6 Address	IPv6 address of the WAN port (if IPv6 is enabled).
State	Shows if the WAN port is active or inactive for routing. If the WAN port is active for routing, the WAN state shows "Up." If the WAN port is inactive for routing, the WAN state shows "Down." **NOTE** The state "Down" means that the network detection fails.
Wireless	
Displays the status of all four predefined SSIDs. To view complete wireless settings, click **details**. See **Viewing Wireless Statistics** for more information.	
Signal Strength	Shows if the Wi-Fi signal strength is 100%, 50%, or off.
cisco-xxxx	Shows if the predefined SSID is enabled or disabled.
VPN	
QuickVPN Users	Number of QuickVPN users.

Viewing System Summary

The System Summary page displays a summary of the CVR100W's settings.

To view a summary of system settings:

STEP 1 Choose **Status** > **System Summary**.

STEP 2 From the **Refresh Rate** drop-down menu, choose a refresh rate.

The System Summary page displays the following information:

System Information	
Firmware Version	Firmware version that the CVR100W is currently using.
Firmware MD5 Checksum	Message-Digest algorithm used to verify the integrity of files.
System Up Time	Duration for which the system has been running.
Current Time	Time of day.
PID VID	Product ID and version ID of the CVR100W.
IPv4 Configuration	
LAN IP	LAN address of the CVR100W.
WAN IP	WAN address of the CVR100W. When the WAN port is configured to obtain an IP address from your ISP using Dynamic Host Configuration Protocol (DHCP), you can click **Release** to release its IP address, or click **Renew** to obtain a new IP address.
Gateway	IP address of default network gateway.
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.
DNS 3	Third DNS server IP address of the WAN port.
DDNS	Shows if the Dynamic DNS (DDNS) is enabled or disabled.
IPv6 Configuration (if IPv6 address mode is enabled)	
LAN IP	LAN address of the CVR100W.
WAN IP	WAN address of the CVR100W.
Gateway	IP address of default network gateway.

DNS 1	IP address of the primary DNS server.
Wireless Summary	
SSIDx	Name of the wireless network.
Security	Security setting for the wireless network.
Firewall Setting Status	
DoS (Denial of Service)	Shows if DoS protection is on or off.
Block WAN Request	Shows if WAN request blocking is on or off.
Remote Management	Shows if remote management is on or off.
VPN Setting Status	
Available QuickVPN Connections	Number of available QuickVPN connections.
Connected QuickVPN Users	Number of connected QuickVPN users.

Viewing Connected Devices

The Connected Devices page displays information about the active devices connected to the CVR100W.

NOTE The Connected Devices page displays information from devices that have responded to the CVR100W's Address Resolution Protocol (ARP) request. If a device does not respond to the request, it is removed from the list.

To view connected devices:

STEP 1 Choose **Status** > **Connected Devices**.

STEP 2 To specify the types of interfaces to display, choose an option from the **View according to interface type** drop-down menu. You can choose one of the following options:

All	Displays a list of all devices connected to the CVR100W.
Wireless	Displays a list of all wireless devices connected to the CVR100W.
Wired	Displays a list of all devices connected through the Ethernet ports on the CVR100W.
WDS	Displays a list of all Wireless Distribution System (WDS) devices connected to the CVR100W.

The **ARP** table displays the following information:

Name	Name of the device connected to the CVR100W.
IP Address	IP address of the connected device.
MAC Address	MAC address of the connected device.
Type	Connection type of the connected device.
Static DHCP	Shows if Static DHCP is enabled or disabled on the connected device.
Interface Type	Device interface type, such as Wired, WDS, and so on.

Viewing DHCP Leased Clients

To view information for the DHCP clients:

STEP 1 Choose **Status** > **DHCP Leased Clients**.

For every VLAN defined on the CVR100W, this page displays a list of the clients associated with the VLAN.

Host Name	Name of the device connected to the CVR100W.

IP Address	IP Address of the connected device.
MAC Address	MAC Address of the connected device.
Static DHCP Binding	Check to enable Static DHCP Binding for this device. The CVR100W will always assign this IP address to the device.

STEP 2 Click **Save** to apply your settings.

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 CVR100W 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 round-up form, check **Show Simplified Statistic Data** and click **Save**.

STEP 4 To reset the port statistics counters, click **Clear Counters**.

The Port Statistics table displays the data transfer statistics for the WAN, LAN, and WLAN ports:

Interface	Name of the network interface.
Packet	Number of the received and sent packets through the interface.
Byte	Number of the received and sent bytes of information per second.
Error	Number of the received and sent packet errors.

Dropped	Number of the received and sent packets that were dropped.
Multicast	Number of multicast packets sent over this radio.
Collisions	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 Wireless Statistics

The Wireless Statistics page shows a cumulative total of relevant wireless statistics for the radio on the CVR100W.

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 round-up form, check **Show Simplified Statistic Data** and click **Save**.

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

The Wireless Statistics table displays the following information:

SSID Name	Name of the wireless network.
Packet	Number of received and sent wireless packets for each SSID, and total number of received and sent wireless packets for all SSIDs.
Byte	Number of received and sent bytes of information for each SSID, and total number of received and sent bytes of information for all SSIDs.

Error	Number of received and sent packet errors for each SSID, and total number of received and sent packet errors for all SSIDs.
Dropped	Number of received and sent packets dropped by each SSID, and total number of received and sent packets dropped by all SSIDs.
Multicast	Number of multicast packets sent over each SSID, and total number of multicast packets sent over all SSIDs.
Collisions	Number of packet collisions reported to each SSID, and total number of packet collisions for all SSIDs.

Viewing Guest Network Status

The Guest Network Status page displays information for all wireless guests connected to the SSID4 of the CVR100W.

Up to ten wireless guests can be allowed to simultaneously connect to the SSID4. The default value is five. The CVR100W will block the new requests when the number of the connected guests reaches the limitation. A warning message will be appeared at this time.

The CVR100W limits the time (two hours) that each guest can be connected to the SSID4. The guest connection will be terminated over the time limit. You can also manually terminate the guest connection at any time.

To view guest network status:

STEP 1 Choose **Status** > **Guest Network Status**.

The Guest Network Status table displays the following information:

Host Name	Name of the device connected to the SSID4 of the CVR100W.
IP Address	IP address of the connected device.
MAC Address	MAC address of the connected device.

Time Left	Time left for the guest connection.
Status	Shows if the device is connected to the Internet using the CVR100W.

STEP 2 To manually disconnect the guest connection, click **Disconnect**.

Viewing VPN Status

The VPN Status page displays the status of client-to-gateway VPN connections.

To view VPN user connection status:

STEP 1 Choose **Status** > **VPN Status**.

The VPN User Connection Status table displays the following information:

Username	Username of the VPN user associated with the QuickVPN tunnel.
Remote IP	IP address of the remote QuickVPN client. This could be a NAT/Public IP if the client is behind the NAT router.
Status	Current status of QuickVPN client. OFFLINE means that the QuickVPN tunnel is not initiated or established by the VPN user. ONLINE means that the QuickVPN tunnel, initiated or established by the VPN user, is active.
Start Time	Time of the VPN user establishing a connection.
End Time	Time of the VPN user ending a connection.
Duration (Seconds)	Duration between the VPN user establishing and ending a connection.
Protocol	Protocol that the user uses, such as QuickVPN.

STEP 2 To manually terminate a VPN session, click **Disconnect**.

Viewing Logs

The View Logs page allows you to view the CVR100W 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.
Information	Device information.
Debugging	Provides detailed information about an event.

The System Log table displays the following information:

Log Index	Index number of the log.
Log Time	Time of the log.
Log Severity	Severity of the log.

Description	Description of the log.

STEP 4 To delete all entries in the table, click **Clear Logs**.

STEP 5 To save all log messages to your local PC, click **Save Logs**.

STEP 6 To specify the number of entries to show per log, choose a number from the drop-down menu.

STEP 7 Use the page navigation buttons to move between log pages.

Viewing IPsec Connection Status

The IPSec Connection Status page displays the status of all site-to-site VPN policies on the CVR100W. 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 From the **Refresh Rate** drop-down menu, choose a refresh rate. This action causes the page to reread the status and statistics from the CVR100W 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**.

In the **Active IPSec Security Association Table**, the following information for each site-to-site VPN policy is displayed:

Policy Name	Name of the VPN policy for which data is displayed.
Local	Local IP address.
Remote	Remote IP address.
Start Time	Start time of the IPsec VPN connection.
End Time	End time of the IPsec VPN connection.

Duration	Elapsed time for which the connection is or was active.
Packet	Received (Rx) and transmitted (Tx) packets on the connection.
Byte	Received (Rx) and transmitted (Tx) bytes on the connection.
State	State of the connection (for example, active or not connected).

STEP 4 Click **Connect** to manually establish a VPN connection, or click **Disconnect** to manually terminate an active VPN connection.

Viewing CSC Information

The CSC Information page displays the status for all wireless clients that are associated with the Cisco Simple Connect (CSC) wireless network of the CVR100W.

To view information for all CSC wireless clients:

STEP 1 Choose **Status** > **CSC Information**.

The following information for each CSC wireless client is displayed:

MAC Address	MAC address of the connected wireless client.
Login Mode	Method how the wireless client connects to the CSC wireless network of the CVR100W.
Leave Time	Remaining online time for this wireless client if the CVR100W limits the time to access the Internet.

STEP 2 Click **Disconnect** to manually terminate a CSC wireless connection.

Viewing NETSTAT Information

The NETSTAT page displays information for all active Internet connections.

To see complete details for active Internet connections, click **Status** > **NETSTAT**. The following information is displayed:

Proto	The protocol (TCP, UDP, or raw) used by the socket.
Recv-Q	The count of bytes not copied by the user program connected to this socket.
Send-Q	The count of bytes not acknowledged by the remote host.
Local Address	Address and port number of the local end of the socket.
Foreign Address	Address and port number of the remote end of the socket.

State	The state of the socket. Since there are no states in raw mode and usually no states used in UDP, this column may be left blank. Normally this can be one of several values: ▪ **ESTABLISHED:** The socket has an established connection. ▪ **SYN_SENT:** The socket is actively attempting to establish a connection. ▪ **SYN_RECV:** A connection request has been received from the network. ▪ **FIN_WAIT1:** The socket is closed, and the connection is shutting down. ▪ **FIN_WAIT2:** The connection is closed, and the socket is waiting for a shutdown from the remote end. ▪ **TIME_WAIT:** The socket is waiting after close to handle packets still in the network. ▪ **CLOSED:** The socket is not being used. ▪ **CLOSE_WAIT:** The remote end has shut down, waiting for the socket to close. ▪ **LAST_ACK:** The remote end has shut down, and the socket is closed. Waiting for acknowledgement. ▪ **LISTEN:** The socket is listening for incoming connections. Such sockets are not included in the output unless you specify the --listening (-l) or --all (-a) option. ▪ **CLOSING:** Both sockets are shut down but we still do not have all our data sent. ▪ **UNKNOWN:** The state of the socket is unknown.

3

Configuring Network

This chapter describes how to configure the CVR100W's network settings. It includes the following sections:

- **Configuring WAN Settings**
- **Configuring LAN Settings**
- **Configuring Routing**
- **Configuring Dynamic DNS**
- **Configuring IP Mode**
- **Configuring IPv6**

Configuring WAN Settings

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

The Internet Setup page allows you to configure how to connect the WAN interface to the Internet. The CVR100W supports four types of Internet connections:

- **Configuring Automatic Configuration (DHCP)**
- **Configuring PPPoE**
- **Configuring Static IP**
- **Configuring Optional Settings**

Sometimes, you may need to set the MAC address of the CVR100W's WAN port to be the same MAC address as your PC's or some other MAC address.

- **Cloning the MAC Address**

Configuring Automatic Configuration (DHCP)

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

To configure the DHCP settings:

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

STEP 2 From the **Internet Connection Type** drop-down menu, choose **Automatic Configuration - DHCP**.

STEP 3 (Optional) To configure other optional settings, see **Configuring Optional Settings**.

STEP 4 Click **Save**.

Configuring PPPoE

To configure the PPPoE settings:

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

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

STEP 3 In the **PPPoE Settings** area, enter the following information (you may need to contact your ISP to obtain your PPPoE login information):

Username	Enter your username assigned to you by the ISP.
Password	Enter your password assigned to you by the ISP.
Connect on Demand	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 **Connect on Demand**, enter the number of minutes after which the connection shuts off in the **Max Idle Time** field.

Keep Alive	When you select this option, the Internet connection is always on. If you click **Keep Alive**, enter the number of seconds that the CVR100W attempts to reconnect after it is disconnected in the **Redial period** field.
Authentication Type	Choose the authentication type: ▪ **Auto Negotiation:** The server sends a configuration request specifying the security algorithm set on it. Then, the CVR100W sends back authentication credentials with the security type sent earlier by the server. ▪ **PAP:** The CVR100W uses the Password Authentication Protocol (PAP) to connect to the ISP. ▪ **CHAP:** The CVR100W uses the Challenge Handshake Authentication Protocol (CHAP) when connecting with the ISP. ▪ **MS-CHAP or MS-CHAPv2:** The CVR100W uses Microsoft Challenge Handshake Authentication Protocol when connecting with the ISP.

STEP 4 (Optional) To configure other optional settings, see **Configuring Optional Settings**.

STEP 5 Click **Save**.

Configuring Static IP

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

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

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

STEP 3 In the **Static IP Settings** area, enter the following information:

Internet IP Address	Enter the IP address of the WAN port.
Subnet Mask	Enter subnet mask of the WAN port.
Default Gateway	Enter the IP address of the default gateway.
Static DNS 1	Enter the IP address of the primary DNS server.
Static DNS 2	Enter the IP address of the secondary DNS server.

STEP 4 (Optional) To configure other optional settings, see **Configuring Optional Settings**.

STEP 5 Click **Save**.

Configuring Optional Settings

To configure optional WAN settings:

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

STEP 2 In the **Optional Settings** area, enter the following information:

Host Name	Enter the host name of the CVR100W.
Domain Name	Enter the domain name for your network.
MTU	The Maximum Transmit Unit (MTU) is the size of the largest packet that can be sent over the network. The standard MTU value for Ethernet networks is usually 1500 bytes. For PPPoE connections, the value is 1492 bytes. Unless a change is required by your ISP, Cisco recommends that you choose **Auto**. The default MTU size is 1500 bytes. If your ISP requires a custom MTU setting, choose **Manual** and enter the MTU size.
Size	Enter the MTU size.

STEP 3 Click **Save**.

Cloning the MAC Address

Sometimes, you may need to set the MAC address of the CVR100W's WAN port to be the same MAC address as your PC's or some other MAC address. This is called MAC address cloning.

For example, some ISP registers your computer's 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 CVR100W's WAN port is not recognized by the ISP.

In this case, to configure your CVR100W to be recognized by the ISP, clone the MAC address of the WAN port to be the same as your computer's MAC address.

To configure a MAC address clone:

STEP 1 Choose **Networking** > **WAN** > **MAC Address Clone**.

STEP 2 In the **MAC Address Clone** field, check **Enable** to enable MAC address cloning.

STEP 3 Set the MAC address of the CVR100W's WAN port, do one of the following:

- To set the MAC address of the WAN port to your PC's 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 LAN Settings

The default DHCP and TCP/IP settings work for most applications. You can assign an IP address to each additional logical subnet on the CVR100W.

Configuring Basic LAN Settings

You can configure the CVR100W's IP address and DHCP settings.

IPv4

To configure the default LAN IP address of the CVR100W:

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

STEP 2 In the **IPv4** area, enter the following information:

VLAN	Choose the VLAN number from the drop-down menu.
Local IP Address	Enter the LAN IP address of the CVR100W. Make sure the address is not in use by another device.
Subnet mask	Choose the subnet mask for the new IP address from the drop-down menu. The default subnet is 255.255.255.0.

STEP 3 Click **Save**.

After the CVR100W's LAN IP address is changed, your PC is no longer connected to the CVR100W.

STEP 4 To reconnect your PC to the CVR100W, do one of the following:

- If DHCP is configured on the CVR100W, release and renew your PC's IP address.
- Manually assign an IP address to your PC. The address must be on the same subnet as the CVR100W. For example, if you change the CVR100W's IP address to 10.0.0.1, assign your PC an IP address in the range of 10.0.0.2 to 10.0.0.255.

STEP 5 Open a new browser window and enter the new IP address of the CVR100W to reconnect.

Configuring DHCP

By default, the CVR100W 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 CVR100W's IP address serves as the gateway address to your LAN. The CVR100W assigns IP addresses to PCs on the LAN from a pool of addresses. The CVR100W tests each address before it is assigned to avoid duplicate addresses on the LAN.

By default, the CVR100W 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 the DHCP settings:

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

STEP 2 (Optional) Select the VLAN that you want to edit from the drop-down menu.

STEP 3 In the **DHCP Server** field, select one of the following options:

Enable	Click this radio button to allow the CVR100W to act as the DHCP server in the network.
Disable	Click this radio button to disable DHCP on the CVR100W. If you want another device on your network to be the DHCP server, or to manually configure the network settings of all of your PCs, disable DHCP.
DHCP Relay	Click this radio button to select DHCP Relay to configure the CVR100W to act as a relayer of IP addresses by a different DHCP server.

STEP 4 If you select **Enable**, enter the following information:

Starting IP Address	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 that you enter in the **Maximum Number of DHCP Users** field).
Maximum Number of DHCP Users	Enter the maximum number of DHCP clients.
IP Address Range	(Read-only) Displays the range of IP addresses available to the DHCP clients.
Client Lease time	Enter the duration (in hours) for which IP addresses are leased to clients.
Static DNS 1	Enter the IP address of the primary DNS server.
Static DNS 2	Enter the IP address of the secondary DNS server.
Static DNS 3	Enter the IP address of the tertiary DNS server.
WINS	Enter the IP address of the primary WINS server.

STEP 5 If you select **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 VLAN

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.

To create a VLAN:

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

STEP 2 Click **Add Row**.

STEP 3 Enter the following information:

VLAN ID	Enter the numerical VLAN ID to assign to endpoints in the VLAN membership. The number that you enter must be between 4 and 15. VLAN ID 1 is reserved for the default VLAN, which is used for untagged frames received on the interface. VLAN ID 2 is reserved cannot be used. VLAN ID 3 is reserved for the guest network.
Description	Enter a description to identify the VLAN.
Port 1 **Port 2** **Port 3** **Port 4**	You can associate VLANs on the CVR100W 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: ▪ **Untagged:** The port is an untagged member of the VLAN. Frames of the VLAN are sent untagged to the port VLAN. ▪ **Tagged:** The port is a tagged member of the VLAN. Frames of the VLAN are sent tagged to the port VLAN. ▪ **Excluded:** The port is currently not a member of the VLAN. This is the default for all the ports when the VLAN is first created.

STEP 4 Click **Save**.

STEP 5 To edit the settings of a VLAN, select the VLAN and click **Edit**. To delete a selected VLAN, click **Delete**. Click **Save** to apply your changes.

Configuring Static DHCP

You can configure the CVR100W 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 the following information:

Description	Enter a description of the client.
IP Address	Enter the IP address of the device. The assigned IP address should be outside the pool of the DHCP addresses configured. The DHCP pool is treated as a generic pool and all reserved IPs should be outside this pool. Static DHCP assignment means that 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.
MAC Address	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).

STEP 5 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 your changes.

Configuring a DMZ Host

The CVR100W 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 recommended 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 CVR100W's 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 VLAN where DMZ is enabled.

STEP 4 In the **Host IP Address** field, enter the IP address of the DMZ host.

STEP 5 Click **Save**.

Configuring Routing

Configuring Operating Mode

To configure the CVR100W's operating mode:

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

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

Gateway	(Recommended) Click this radio button to set the CVR100W to act as a gateway. Keep this default setting if the CVR100W is hosting your network's connection to the Internet.
Router	Click this radio button to set the CVR100W to act as a router. Select this option if the CVR100W is on a network with other routers. Enabling the Router mode disables NAT (Network Address Translation) on the CVR100W.

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 enables the CVR100W to automatically adjust to physical changes in the network's 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.

NOTE RIP is disabled by default on the CVR100W.

To configure dynamic routing:

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

STEP 2 In the **Dynamic Routing** area, configure the following settings:

RIP	Check **Enable** to enable RIP. This allows the CVR100W to use RIP to route traffic.

RIP Send Packet Version	Select the RIP Send Packet Version (**RIPv1** or **RIPv2**). The version of RIP used to send routing updates to other routers on the network depends on the configuration settings of the other routers. It is best to check with your network administrator to see which version of RIP is supported on your network. RIPv2 is backward compatible with RIPv1.
RIP Recv Packet Version	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.

CAUTION Be careful not to introduce routing loops in your network.

To configure static routing:

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

STEP 2 In the **Static Routing** area, choose a route entry from the **Route Entries** drop-down menu.

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

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

Enter Route Name	Enter the name of the route.
Destination LAN IP	Enter the IP address of the destination LAN.
Subnet Mask	Enter the subnet mask of the destination network.
Gateway	Enter the IP address of the gateway used for this route.
Interface	Select the interface to which packets for this route are sent: ▪ **LAN:** Click this radio button to direct packets to the LAN. ▪ **WAN:** Click this radio button to direct packets to the Internet (WAN).

STEP 4 Click **Save**.

Configuring Inter-VLAN Routing

To configure inter-VLAN routing:

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

STEP 2 In the **Inter-VLAN Routing** area, check **Enable** to enable inter-VLAN routing.

STEP 3 Click **Save**.

Viewing the Routing Table

To show the routing table:

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

STEP 2 To view the IPv4 routing information on your network, click **Show IPv4 Routing Table** in the **Routing Table** area.

STEP 3 To view the IPv6 routing information on your network, click **Show IPv6 Routing Table** in the **Routing Table** area.

The routing table displays the following information:

Destination LAN IP	(IPv4) IP address of the destination LAN.
Subnet Mask	(IPv4) Subnet mask of the destination network.
Gateway	(IPv4) IP address of the gateway used for this route.
Interface	(IPv4) Physical network interface through which this route is accessible.
Destination	(IPv6) IP address of the destination LAN.
Next Hop	(IPv6) IP address of the gateway/router through which the destination host/network can be reached.
Interface	(IPv6) Physical network interface through which this route is accessible.

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 oray.org or 3322.org.

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 the following information:

Username	Enter the username of the DDNS account.

Password	Enter the password of the DDNS account.
Host Name	(3322.org) Enter the host name of the DDNS server.
Internet IP Address	(3322.org) Internet IP address of the CVR100W.
Status	(3322.org) Displays the status if the DDNS update has completed successfully or if the account update information sent to the DDNS server failed.
Domain Name	(oray.org) Displays the domain name of the account.
User Level	(oray.org) Displays the user level of the account.
Status	(oray.org) Displays the status 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 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.

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:

LAN:IPv4, WAN:IPv4	Choose this option to use IPv4 in the LAN and WAN ports.
LAN:IPv6, WAN:IPv4	Choose this option to use IPv6 in the LAN ports and IPv4 in the WAN ports.
LAN:IPv6, WAN:IPv6	Choose this option to use IPv6 in the LAN and WAN ports.

LAN:IPv4+IPv6, WAN:IPv4	Choose this option to use IPv4 and IPv6 in the LAN ports and IPv4 in the WAN ports.
LAN:IPv4+IPv6, WAN:IPv4+IPv6	Choose this option to use IPv4 and IPv6 in the LAN and 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:

- Click **Show Static 6to4 DNS Entry**.
- In the **Domain** and **IP** fields, enter up to 5 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

Configuring IPv6 WAN Settings

Configuring WAN properties for an IPv6 network depends on the type of internet connection that you have. You can configure the CVR100W 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 CVR100W, you must first set the IP mode to LAN:IPv6, WAN:IPv6 or LAN:IPv4+IPv6, WAN:IPv4+IPv6.

See **Configuring IP Mode** for more information.

Configuring DHCPv6

If your ISP provides you with a dynamically assigned address, configure the CVR100W to use be a DHCPv6 client.

To configure the CVR100W to be a DHCPv6 client:

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

STEP 2 In the **WAN Connection Type** field, click the **Automatic Configuration-DHCPv6** radio button.

STEP 3 Click **Save**.

Configuring a Static IP Address

If your ISP assigns you a fixed address to access the Internet, configure the CVR100W to use a static IPv6 address.

To configure the CVR100W to use a static IPv6 address:

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

STEP 2 In the **WAN Connection Type** field, click the **Static IPv6** radio button.

STEP 3 In the **Static IP Address** area, enter the following information:

IPv6 Address	Enter the IPv6 address of the WAN port.
IPv6 Prefix Length	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's addresses in this field.
Default IPv6 Gateway	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.

Static DNS 1	Enter the IP address of the primary DNS server on the ISP's IPv6 network.
Static DNS 2	Enter the IP address of the secondary DNS server on the ISP's IPv6 network.

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 CVR100W, 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 IP Mode** for more information.

Configuring IPv6 LAN Settings

To configure IPv6 LAN settings:

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

STEP 2 In the **IPv6** area, enter the following information to configure the IPv6 LAN address:

IPv6 Address	Enter the IPv6 address of the CVR100W. The default IPv6 address for the gateway is fec0::1. You can change this 128-bit IPv6 address based on your network requirements.

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

STEP 3 Click **Save**.

Configuring DHCPv6 Settings

To configure DHCPv6 settings:

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

STEP 2 In the **Server Settings (DHCPv6)** area, enter the following information to configure the DHCPv6 settings:

DHCP Status	Check to enable the DHCPv6 server. If enabled, the CVR100W assigns an IP address within the specified range plus additional specified information to any LAN endpoint that requests DHCP-served addresses.
Domain Name	Enter the domain name of the DHCPv6 server.
Server Preference	Enter the server preference level of this DHCP server. DHCP advertise messages with the highest server preference value to a LAN host are preferred over other DHCP server advertise messages. The default is 255.
Static DNS 1	Enter the IPv6 address of the primary DNS server on the ISP's IPv6 network.
Static DNS 2	Enter the IPv6 address of the secondary DNS server on the ISP's IPv6 network.

Client Lease Time	Enter the client lease time. Enter the duration for which IPv6 addresses are leased to endpoints on the LAN.

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 CVR100W's DHCPv6 server. Using a delegation prefix, you can automate the process of informing other networking equipment on the LAN of DHCP information specific for the assigned prefix.

To configure IPv6 address pools:

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

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

STEP 3 Enter the following information:

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

STEP 4 Click **Save**.

STEP 5 To edit the settings of a pool, select the pool and click **Edit**. To delete a selected pool, click **Delete**. Click **Save** to apply your 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 an IPv6 static route:

STEP 1 Choose **Networking** > **IPv6 Configuration** > **IPv6 Static Routing**.

STEP 2 In the **IPv6 Static Routing** table, click **Add Row**.

STEP 3 Enter the following information:

Name	Enter the route's name.
Destination	Enter the IPv6 address of the destination host or network for this route.
Prefix Length	Enter the number of prefix bits in the IPv6 address that define the destination subnet.
Gateway	Enter the IPv6 address of the gateway through which the destination host or network can be reached.
Interface	Choose the interface for the route from the drop-down menu: **LAN**, **WAN**, or **6to4**.
Metric	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.

Active	Check to make the route active. When you add a route in an inactive state, it gets listed in the routing table, but is not used by the CVR100W. You can always activate the route later. This feature is useful if the network that the route connects to is not available when you added the route. When the network becomes available, you can enable the route.

STEP 4 Click **Save**.

STEP 5 To edit the settings of a route, select the route and click **Edit**. To delete a selected route, click **Delete**. Click **Save** to apply your 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 CVR100W, RIPng is disabled by default.

To configure RIPng:

STEP 1 Choose **Networking** > **IPv6 Configuration** > **Routing (RIPng)**.

STEP 2 Check **Enable**.

STEP 3 Click **Save**.

Configuring IPv6-to-IPv4 Tunneling

IPv6-to-IPv4 tunneling (6-to-4 tunneling) allows IPv6 packets to be transmitted over an IPv4 network. 6to4 tunneling is typically used when a site or end user wants to connect to the IPv6 Internet using the existing IPv4 network.

To configure IPv6-to-IPv4 tunneling:

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

STEP 2 Check **Enable**.

STEP 3 Click **Save**.

Viewing IPv6 Tunnel Status

To view IPv6 tunnel status:

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

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.

STEP 2 Click **Refresh** to refresh the data on this page.

Configuring Router Advertisement

The Router Advertisement Daemon (RADVD) on the CVR100W listens for router solicitations in the IPv6 LAN and responds with router advertisements as required. This is stateless IPv6 auto configuration, and the CVR100W distributes IPv6 prefixes to all nodes on the network.

To configure the RADVD:

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

STEP 2 Enter the following information:

RADVD Status	Check **Enable** to enable RADVD, or check **Disable** to disable RADVD.
Advertise Mode	Select one of the following modes: ▪ **Unsolicited Multicast:** Select this mode to send Router Advertisements (RAs) to all interfaces belonging to the multicast group. ▪ **Unicast Only:** Select this mode to restrict advertisements to well-known IPv6 addresses only (RAs are sent to the interface belonging to the known address only).
Advertise Interval	If you choose **Unsolicited Multicast** as the advertise mode, enter the advertise interval (4 to 1800). The default is **30**. The advertise interval is a random value between the Minimum Router Advertisement Interval (MinRtrAdvInterval) and Maximum Router Advertisement Interval (MaxRtrAdvInterval). MinRtrAdvInterval = 0.33 * MaxRtrAdvInterval
RA Flags	Check **Managed** to use the administered/stateful protocol for address auto configuration. Check **Other** to use the administered/stateful protocol of other, non-address information auto configuration.
Router Preference	Choose **low**, **medium**, or **high** from the drop-down menu. The default is **medium**. 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.

MTU	Enter the MTU size (0 or 1280 to 1500). The default is **1500** bytes. 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.
Router Life Time	Enter the router lifetime value, or the time in seconds that the advertisement messages exists on the route. The default is **3600** seconds.

STEP 3 Click **Save**.

Configuring Advertisement Prefixes

To configure the RADVD available prefixes:

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

STEP 2 Click **Add Row**.

STEP 3 Enter the following information:

IPv6 Prefix Type	Choose one of the following types: ▪ **6to4:** 6to4 is a system that allows IPv6 packets to be transmitted over an IPv4 network. It is used when an end user wants to connect to the IPv6 Internet using their existing IPv4 connection. ▪ **Global/Local:** A locally unique IPv6 address that you can use in private IPv6 networks or a globally unique IPv6 Internet address.
SLA ID	If you choose **6to4** as the IPv6 prefix type, enter the Site-Level Aggregation Identifier (SLA ID). The SLA ID in the 6to4 address prefix is set to the interface ID of the interface on which the advertisements are sent.

IPv6 Prefix	If you choose **Global/Local** as the IPv6 prefix type, enter the IPv6 prefix. The IPv6 prefix specifies the IPv6 network address.
IPv6 Prefix Length	If you choose **Global/Local** 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.
Prefix Lifetime	Enter the prefix lifetime, or the length of time over which the requesting router is allowed to use the prefix.

STEP 4 Click **Save**.

4

Configuring Wireless Network

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

- **Wireless Security**
- **CVR100W Wireless Networks**
- **Configuring Basic Wireless Settings**
- **Configuring Advanced Wireless Settings**
- **Configuring WDS**
- **Configuring WPS**

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's 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 off wireless routers, access points, or gateways when they are not 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.

CVR100W Wireless Networks

The CVR100W provides four virtual wireless networks or four SSIDs (Service Set Identifier).

This table describes the default settings of these networks:

SSID Name	cisco-xxxx	cisco-SSID2	cisco-SSID3	cisco-guest
Enabled	Yes	No	No	No
SSID Broadcast	Enabled	Disabled	Disabled	Enabled
Security Mode	WPA2 mixed	Disabled	Disabled	Disabled
MAC Filter	Disabled	Disabled	Disabled	Disabled
VLAN	1	1	1	3

SSID Name	cisco-xxxx	cisco-SSID2	cisco-SSID3	cisco-guest
SSID Isolation	Disabled	Disabled	Disabled	Enabled
WMM	Enabled	Enabled	Enabled	Enabled
WPS Hardware Button	Enabled	Disabled	Disabled	Disabled

Configuring Basic Wireless Settings

The Basic Settings page allows you to configure basic wireless settings.

Configuring Wireless Radio Settings

To configure the wireless radio settings:

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

STEP 2 In the **Radio** field, check **Enable** to turn the wireless radio on.

This field enables the wireless radio itself. By default there is only one wireless network enabled, cisco-xxxx.

STEP 3 In the **Wi-Fi Power** field, select the Wi-Fi power on your network.

STEP 4 In the **Wireless Network Mode** field, choose one of these options from the drop-down menu:

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

B/G-Mixed	Choose this option if you have Wireless-B and Wireless-G devices in your network.
G/N-Mixed	Choose this option if you have Wireless-G and Wireless-N devices in your network.

STEP 5 In the **Wireless Band Selection** field, choose either **20MHz** or **20/40MHz** as the wireless bandwidth on your network.

STEP 6 In the **Wireless Channel** field, choose the wireless channel from the drop-down menu or choose **Auto** to let the system determine the optimal channel to use based on the environmental noise levels for the available channels.

STEP 7 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 CVR100W's Configuration Utility.

STEP 8 (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 percent and minimize transmit delays.

STEP 9 Click **Save**.

Configuring Wireless Network Settings

The **Wireless Table** in the Basic Settings page lists the settings of the four wireless networks supported on the CVR100W.

To configure the settings for a wireless network:

STEP 1 Check the box for the network that you want to configure, and click the **Edit** button.

STEP 2 Configure these settings:

Enable SSID	Check to enable the wireless network.
SSID Name	Enter the name of the wireless network.
SSID Broadcast	Check to enable SSID broadcast.
Security Mode	(Read Only) Displays the current security settings of the SSID. Refer to the **Configuring Wireless Security** section to modify the security settings of the SSID.
MAC Filter	(Read Only) Displays whether MAC Filter is enabled or disabled. Refer to the **Configuring MAC Address Filtering** section to enable or disable this feature on the SSID.
CSC	(Only applicable for SSID1, SSID2, and SSID3) Check to set this SSID as the Cisco Simple Connect (CSC) wireless access point. Refer to the **Configuring Cisco Simple Connect** section for more information about the Cisco Simple Connect (CSC) feature.
VLAN	Choose the VLAN associated with the network.
SSID Isolation	Check to enable wireless isolation within the SSID.
WMM (Wi-Fi Multimedia)	Check to enable WMM.
WPS Hardware Button	Check to map the CVR100W's WPS button on the front panel to this network.

STEP 3 Click **Save**.

Configuring Wireless Security

For security purposes, we strongly recommend that you configure each SSID with the highest level of security that is supported by the devices into your wireless network. You can configure one of the following security modes for the wireless network:

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. If you do not have to use WEP, we recommend that you use WPA2.

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 Pre-shared 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.

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 security settings for a SSID:

STEP 1 In the **Wireless Table** (**Wireless** > **Basic Settings**), check the SSID that you want to configure.

STEP 2 Click **Edit Security Mode**. The Security Settings page opens.

STEP 3 From the **Security Mode** menu, choose a security mode and specify the corresponding settings. The following table lists the security settings for different security modes.

Disabled	
If you choose this option, any wireless device that is in range can connect to the SSID. This is the default setting but not recommended. This mode means that any data transferred to and from the SSID is not encrypted. This security mode can be useful during initial network configuration or for problem solving, but it is not recommended for regular use on the internal network because it is not secure.	
WEP	
Authentication Type	Choose **Open System** or **Shared Key** if your network administrator recommends this setting. If you are unsure, select the default option (Open System). In both cases, the wireless client must provide the correct shared key (password) to access the wireless network.
Encryption	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.
Passphrase	(Optional) Enter an alphanumeric phrase (longer than eight characters for optimal security) and click **Generate** to generate four unique WEP keys in the **Key1-4** 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.

Show Password	Check to show the password in plaintext.
WPA-Personal, WPA2-Personal, or WPA2-Personal Mixed	
Encryption	For WPA-Personal, 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. WPA2-Personal always uses AES for data encryption. WPA2-Personal Mixed automatically uses TKIP or AES for data encryption.
Security Key	Enter an alphanumeric phrase (8 to 63 ASCII characters or 64 hexadecimal digits).
Show Password	Check to show the password in plaintext.
Key Renewal	Enter the duration of time (600 to 7200 seconds) between key renewals. The default value is 3600.
WPA-Enterprise, WPA2-Enterprise, or WPA2-Enterprise Mixed	
Encryption	For WPA-Enterprise, 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. WPA2-Enterprise always uses AES for data encryption. WPA2-Enterprise Mixed automatically uses TKIP or AES for data encryption.
RADIUS Server	Enter the IP address of the RADIUS server.
RADIUS Port	Enter the port used to access the RADIUS server.
Shared Key	Enter an alphanumeric phrase (8 to 63 ASCII characters or 64 hexadecimal digits).

Key Renewal	Enter the duration of time (600 to 7200 seconds) between key renewals. The default value is 3600.

STEP 4 Click **Save**.

STEP 5 Click **Back** to go back to the Basic Settings page.

Configuring MAC Address Filtering

You can use MAC address 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 address filtering for each network or SSID.

To configure MAC address filtering:

STEP 1 In the **Wireless Table** (**Wireless** > **Basic Settings**), check the SSID that you want to configure.

STEP 2 Click **Edit MAC Filtering**. The Wireless MAC Filtering page opens.

STEP 3 In the **Wireless MAC Filtering** field, check **Enable** to enable MAC address 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 If you want to add a device in the client list to the **MAC Address Table**, check the box in the **Save to MAC Address Filter List** column and click **Add to MAC** to add the selected device to the **MAC Address Table**.

STEP 7 Click **Save**.

STEP 8 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 SSID that you want to configure.

STEP 2 Click **Time of Day Access**. The Time of Day Access page opens.

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**.

STEP 6 Click **Back** to go back to the Basic Settings page.

Configuring Guest Net

The SSID4 (default name: cisco-guest) is used for guest access. The guests can access the Internet through this SSID and the internal network security would not be affected.

To configure the Guest Net settings:

STEP 1 In the **Wireless Table** (**Wireless** > **Basic Settings**), check SSID 4.

STEP 2 Click **Edit Guest Net**. The Guest Net Settings page appears.

STEP 3 In the **Guest Password** field, enter an alphanumeric phrase (8 to 63 ASCII characters or 64 hexadecimal digits).

STEP 4 Check **Hide Password** to show the password in ciphertext.

STEP 5 In the **Lease Time** field, set the guest least time. (Range: 1 to 9999 minutes, default: 120 minutes)

STEP 6 In the **Total Guest Allowed** field, set the maximum number of the guest connections allowed.

STEP 7 Click **Save**.

STEP 8 Click **Back** to go back to the Basic Settings page.

Configuring Cisco Simple Connect

Cisco Simple Connect (CSC) provides a safe and convenient way for CSC-enabled devices to connect with a Wi-Fi access point by simply touching the RFiD or scanning the QR code of the CSC card. Cisco Simple Connect makes accessing wireless access points simple and allows you to expand more business applications. See **Using Cisco Simple Connect** for more information.

By default, Cisco Simple Connect (CSC) is disabled on the CVR100W. You can set one of the SSIDs (SSID1, SSID2, or SSID3) of the CVR100W as the CSC wireless access point. The wireless clients that are associated with the CSC wireless access point can only access the Internet through the CVR100W.

When configuring Cisco Simple Connect, note the following:

- Only SSID1, SSID2, or SSID3 can be set as the CSC wireless access point.
- Enabling Cisco Simple Connect on a SSID does not affect the normal operation of other SSIDs.
- SSID1 must be set as the CSC wireless access point when WDS is enabled on the CVR100W.
- The VLAN to which the CSC wireless access point is mapped cannot be the same as the VLANs of other SSIDs. You must assign a different VLAN to the CSC wireless access point.
- When enabling Cisco Simple Connect on a SSID, the CVR100W automatically saves the current settings of the SSID before the CSC settings are applied on the SSID, and restores the saved settings after CSC is disabled on the SSID.
- By default, the CSC wireless access point is automatically named as Cisco-Simple-Connect when enabling Cisco Simple Connect for the first time. The wireless security mode, SSID broadcast, and SSID Isolation are disabled on the CSC wireless access point. For security purposes, we strongly recommend that you configure the CSC wireless access point with the

highest level of security that is supported by the devices into your wireless network.

To enable Cisco Simple Connect and configure the settings of the CSC wireless access point:

STEP 1 Choose **Wireless** > **Basic Settings**. The Basic Settings page opens.

STEP 2 In the Wireless Table, check the SSID that you want to configure and click **Edit**.

STEP 3 Check the **Enable SSID** box to enable this SSID.

STEP 4 Check the **CSC** box to enable Cisco Simple Connect on this SSID.

STEP 5 Select a VLAN from the **VLAN** drop-down menu to which all traffic from the CSC wireless network is mapped. The VLAN that is associated with the CSC wireless network cannot be the same as the VLANs of other SSIDs.

STEP 6 (Optional) Configure the following settings for the CSC wireless access point:

- **SSID Name:** Enter a unique name for the CSC wireless access point. By default, the name of the CSC wireless access point is set to Cisco-Simple-Connect after you enable Cisco Simple Connect for the first time.

  Generally, you can enter the SSID name that is provided on your CSC Simple card in this field. If you want to customize the name of the CSC wireless access point, enter a new SSID name in this field.

  NOTE When you customize a new name of the CSC wireless access point, you are asked to regenerate and print the QR code of the CSC card. See **Customizing Your QR Code** for more information.

- **Security Mode:** By default, the security mode of the CSC wireless access point is disabled. You can modify its security settings by clicking **Edit Security Mode**. For security purposes, we strongly recommend that you configure the CSC wireless access point with the highest level of security that is supported by the devices into your wireless network.

  Generally, you can choose WPA or WPA2 as the security mode and enter the security key that is provided on your CSC card. If you want to customize the security key of the CSC wireless access point, enter a new security key. See **Configuring Wireless Security** for more information.

  NOTE When you customize a new security key of the CSC wireless access point, you are asked to regenerate and print the QR code of the CSC card. See **Customizing Your QR Code** for more information.

- **MAC Filter:** By default, MAC address filtering is disabled on the CSC wireless access point. You can enable this feature and configure the corresponding settings by clicking **Edit MAC Filter**. See **Configuring MAC Address Filtering** for more information.
- **Time of Day Access:** By default, Time of Day Access is disabled on the CSC wireless access point. You can enable this feature and configure the corresponding settings by clicking **Time of Day Access**. See **Configuring Time of Day Access** for more information.
- **SSID Broadcast, WMM, and SSID Isolation:** By default, these features are enabled on the CSC wireless access point. See **Configuring Wireless Network Settings** for more information.

STEP 7 Click **Save**.

STEP 8 Click **Edit CSC** to limit the time to access the Internet for all associated CSC wireless clients.

STEP 9 Enter the following information:

SSID Name	Displays the current name of the CSC wireless access point. By default, it is named as Cisco-Simple-Connect after Cisco Simple Connect is enabled for the first time.
Security Mode	Displays the current security mode used on the CSC wireless access point. By default, the security mode is disabled on the CSC wireless access point.
Security Key	Displays the current security key of the CSC wireless access point.
Show Password	Check the box to display the password in plaintext.
Access Network Time	Enter a value from 0 to 1440 seconds. The default value is 0, which means that there is no limit.

STEP 10 Click **Save**.

See **Connecting to CSC Wireless Network** for more information about how to connect to the CSC wireless network and get the authority to access the Internet.

Configuring Advanced Wireless Settings

CAUTION 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:

Frame Burst	Check Enable to enable this feature 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).
WMM No Acknowledgement	Check **Enable** 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.

Basic Rate	The Basic Rate setting is not the rate of transmission but a series of rates at which the Services Ready Platform can transmit. The CVR100W 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. The default setting is Default, when the CVR100W can transmit at all standard wireless rates (1-2 Mbps, 5.5 Mbps, 11 Mbps, 18 Mbps, 24 Mbps, and so on). In addition to B and G speeds, the CVR100W supports N speeds. Other options are 1-2 Mbps, for use with older wireless technology, and All, when the CVR100W can transmit at all wireless rates. The Basic Rate is not the actual rate of data transmission. If you want to specify the CVR100W's rate of data transmission, configure the Transmission Rate setting.
Transmission Rate	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 Auto to have the CVR100W automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the CVR100W and a wireless client. The default is Auto.

N Transmission Rate	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 Auto to have the CVR100W automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the CVR100W and a wireless client. The default is Auto.
CTS Protection Mode	The CVR100W 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 CVR100W in an environment with heavy 802.11b traffic. This function boosts the CVR100W's ability to catch all Wireless-N and Wireless-G transmissions but will severely decrease performance. The default is Auto.
Beacon Interval	The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the CVR100W to synchronize the wireless network. Enter a value between 40 and 3500 milliseconds. The default value is 100.
DTIM Interval	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. When the CVR100W 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.

Fragmentation Threshold	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. 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.
RTS Threshold	If you encounter inconsistent data flow, enter only minor reductions. The default value of 2347 is recommended. 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. After receiving an RTS, the wireless station responds with a CTS frame to acknowledge the right to begin transmission.

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 CVR100W 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 SSID 1 only.

To configure a WDS:

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

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

STEP 3 To manually enter the MAC address of a repeater, click the **Manual** radio button.

STEP 4 Enter the MAC addresses of up to three access points to use as repeaters in the **MAC 1**, **MAC 2**, **MAC 3** fields.

STEP 5 (Optional) Click the **Show Site Survey** button.

The **Available Networks** table lists the available wireless network access points.

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

STEP 6 Click **Save**.

Configuring WPS

You can configure WPS on the CVR100W to allow WPS-enabled devices to more easily connect to the wireless network.

To enable WPS on your CVR100W:

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

STEP 2 From the **SSID** drop-down menu, choose the wireless network on which the WPS settings are applied.

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

STEP 4 Use one of the following methods to configure WPS on client devices:

- If your client device has a WPS button, first click the WPS button on the client device, and then click the **WPS** button on this page.

- If the client device has a WPS PIN number, enter the PIN number and click **Register**. After configuration is completed, click **OK**.

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

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

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

The status of the WPS light on the front panel provides information about the WPS operation.

WPS Successfully Started	WPS light turns on for 120 seconds.
WPS During Startup	WPS light flashes (0.5 Hz) for 30 seconds.
WPS Errors Occurred	WPS light flashes (1 Hz) for 30 seconds.
WPS Session Overlap	WPS light flashes (0.1 Hz) in one second and turns off next second for 120 seconds.
WPS Enabled or Disabled	WPS light is off.

5

Configuring Firewall

This chapter describes how to configure the firewall settings. It includes the following sections:

- CVR100W Firewall Features
- Configuring Basic Firewall Settings
- Managing Firewall Schedules
- Configuring Service Management
- Configuring Access Control
- Configuring Single Port Forwarding
- Configuring Port Range Forwarding
- Configuring Port Range Triggering

CVR100W Firewall Features

Access Rules

You can secure your network by creating and applying rules that the CVR100W 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 CVR100W should allow or block.
- Direction for the traffic by specifying the source and destination of traffic.
- Schedules as to when the CVR100W should apply rules.

- Keywords (in a domain name or on a URL of a webpage) that the CVR100W should allow or block.
- MAC addresses of devices whose inbound access to your network that the CVR100W should block.
- Port triggers that signal the CVR100W to allow or block access to specified services as defined by port number.

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.

Inbound (WAN to LAN) rules restrict access to traffic entering your network, selectively allowing only specific outside users to access specific local resources. By default, all access from the insecure WAN side is blocked from accessing the secure LAN, except in response to requests from the LAN. 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 CVR100W'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 CVR100W, you may use the IP address if a static address is assigned to the WAN port, or if your WAN address is dynamic, a DDNS (Dynamic DNS) name can be used.

Outbound (LAN to 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 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.

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.

CAUTION 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 CVR100W must send all incoming data for that application only on the required port or range of ports.

The CVR100W 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 Basic Firewall Settings

To configure basic firewall settings:

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

STEP 2 Configure the following firewall settings:

DoS Protection	Check **Enable** to enable Denial of Service (DoS) protection.
Block WAN Request	Check **Enable** to block ping requests to the CVR100W from the WAN.
IPv4 Multicast Passthrough	Check **Enable** to enable multicast passthrough for IPv4.
IPv4 Multicast Immediate Leave	Check **Enable** to enable IGMP proxy immediate leave.

IPv4 Multicast Snooping	Check **Enable** to enable IGMP Snooping.
UPnP	Check **Enable** to enable Universal Plug and Play (UPnP).
Allow Users to Configure	(UPnP) Check 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 CVR100W does not allow application to add the forwarding rule.
Allow Users to Disable Internet Access	(UPnP) Check to allow users to disable Internet access.
Block Java	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. Enabling this setting blocks Java applets from being downloaded. Click **Auto** to automatically block Java, or click **Manual Port** and enter a specific port on which to block Java.
Block Cookies	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. Click **Auto** to automatically block cookies, or click **Manual Port** and enter a specific port on which to block cookies. **NOTE** Many websites require that cookies be accepted in order for the site to be accessed properly. Blocking cookies can cause many websites to not function properly.

Block ActiveX	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. Enabling this setting blocks ActiveX applets from being downloaded. Click **Auto** to automatically block ActiveX, or click **Manual Port** and enter a specific port on which to block ActiveX.
Block Proxy	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. 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. Click **Auto** to automatically block proxy servers, or click **Manual Port** and enter a specific port on which to block proxy servers.

STEP 3 Click **Save**.

Managing Firewall Schedules

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

To create a schedule:

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

STEP 2 Click **Add Row**.

STEP 3 In the **Schedule Name** field, enter a unique name to identify the schedule.

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 boxes 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 choose either **All Times** or **Specific Times**. If you choose **Specific Times**, enter the start and end times.

STEP 6 Click **Save**.

STEP 7 Click **Back** to go back to the Schedule Management page.

STEP 8 To edit an entry, select the entry and click **Edit**. Make your changes, then click **Save**.

Configuring Service 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 Service 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 **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**.

STEP 8 To edit an entry, select the entry and click **Edit**. Make your changes, then click **Save**.

Configuring Access Control

Default Access Control Policy

You can configure the default access control policy for the traffic that is directed from the secure network (LAN) to the non-secure network (dedicated WAN/ optional).

To configure the default access control policy:

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

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

STEP 3 Click **Save**.

Configuring Access Rules

All configured access rules on the CVR100W are displayed in the **Access Rules Table**.

To create an access rule:

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

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:** Blocks the selected type of traffic according to a schedule.
- **Allow by schedule:** Allows the selected type of traffic according to a schedule.

STEP 5 From the **Schedule** drop-down menu, choose the schedule to apply this rule.

(Optional) Click **Configure Schedules** to go to the Schedule Management page to configure the services before applying access rules to them.

STEP 6 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)
- File Transfer Protocol (FTP)
- Hypertext Transfer Protocol (HTTP)
- HTTP Secondary
- Secure Hypertext Transfer Protocol (HTTPS)
- HTTPS Secondary
- 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
- Telnet Secondary

- Telnet SSL
- Voice (SIP)

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

STEP 7 In the **Source IP** field, select the users to which the access 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 IP** 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 IP** field, and the ending IP address in the **Finish** field.

STEP 8 In the **Destination IP** field, select the users to which the access 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 IP** 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 IP** field, and the ending IP address in the **Finish** field.

STEP 9 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 **Always block**, 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.

STEP 10 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 11 In the **Rule Status** field, check to enable the new access rule.

STEP 12 Click **Save**.

STEP 13 Click **Back** to go back to the Access Rules page.

Configuring Internet Access Rules

The CVR100W 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.

To create a Internet access rule:

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

STEP 2 Click **Add Row**.

STEP 3 In the **Rule Status** field, check **Enable** to enable the Internet access rule.

STEP 4 In the **Enter Policy Name** filed, enter a policy name for identification and management purposes.

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

- **Block All:** Block all Internet traffic.
- **Block URL:** Block Internet traffic to specified Internet sites.
- **Block All by Schedule:** Blocks all types of traffic according to a schedule.
- **Block URL by Schedule:** Blocks the specified Internet sites according to a schedule.

STEP 6 If you choose **Block All by Schedule** or **Block URL by Schedule**, choose a schedule from the **Schedule** drop-down menu.

(Optional) Click **Configure Schedules** to go to the Schedule Management page to configure the services before applying the Internet access rules to them.

STEP 7 Apply the Internet access rule to specific PCs. Address filtering allows you to block traffic coming from specific devices.

In the **Apply Access Policy to the Following PCs** table, click **Add Row**.

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).

In the **Value** field, depending on what you chose in the previous step, enter one of the following:

- MAC address (xx:xx:xx:xx:xx:xx) of the PC to which the Internet access rule applies.
- The IP address of the PC to which the Internet access rule applies.
- The starting and ending IP addresses to block (for example, 192.168.1.2 to 192.168.1.30).

STEP 8 In the **Website Blocking** table, click **Add Row**.

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).

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**.

STEP 10 Click **Back** to go back to the Internet Access Rules page.

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 **Service Name** field, enter the name of the service to configure port forwarding for.

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.

STEP 7 In the **Enable** field, check the 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 **Service Name** field, enter the name of the service to configure port forwarding.

STEP 3 In the **Start Port** field, specify the port number that begins the range of ports to forward.

STEP 4 In the **End Port** field, specify the port number that ends the range of ports to forward.

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.

STEP 7 In the **Enable** field, check the box to enable the rule.

STEP 8 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.

To add a port triggering rule:

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

STEP 2 In the **Service Name** field, enter the name of the service to configure port triggering for.

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 box to enable the rule.

STEP 6 Click **Save**.

6

Configuring VPN

This chapter describes how to configure Virtual Private Networks (VPNs) that allow remote workers to access your network resources. It includes the following sections:

- **VPN Tunnel Types**
- **Configuring VPN Clients**
- **Configuring Basic VPN Setup**
- **Configuring Advanced VPN Setup**
- **Managing Certificates**
- **Configuring VPN Passthrough**

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.

Remote Access with Cisco QuickVPN

For quick setup with basic VPN security settings, distribute the 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 in the **VPN** > **VPN Clients** page. See **Configuring VPN Clients**.
2. Instruct users to obtain the free Cisco QuickVPN software from Cisco.com, and install it on their computers. For more information, see **Using Cisco QuickVPN**.

3. To enable access using Cisco QuickVPN on this router, you must enable remote management. See **Configuring Remote Management**.

Site-to-Site VPN

The CVR100W supports site-to-site VPN for a single gateway-to-gateway VPN tunnel. For example, you can configure the CVR100W at a branch site to connect to the router at the corporate site, so that the branch site can securely access the corporate network. See **Configuring Basic VPN Setup** and **Configuring Advanced VPN Setup** for more information on configuring site-to-site VPN.

Configuring VPN Clients

This section describes how to create and manage the QuickVPN users.

Creating and Managing QuickVPN Users

To create QuickVPN users:

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

STEP 2 In the **VPN Client Settings** table, click **Add Row**.

STEP 3 Enter the following information:

Enable	Check to enable the user.
Username	Enter the username of the QuickVPN user (4 to 32 characters). The usernameof the VPN client cannot be same as the name of an existing VPN policy.
Password	Enter the password (4 to 32 characters).
Allow User to Change Password	Check to allow the user to change its password.

STEP 4 Click **Save**.

STEP 5 To edit the settings of a QuickVPN user, check the relative box and click **Edit**. When you are done making changes, click **Save**.

STEP 6 To delete a QuickVPN user, check the relative box and click **Delete**. Then, click **Save**.

Importing VPN Client Settings

You can import the VPN client settings that contain the usernames and passwords of clients from a Comma Separated Value (CSV) text file.

You can first use 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 to import:

PROTOCOL	USERNAME	PASSWORD
QuickVPN	user1	password1
QuickVPN	user2	password2

CAUTION Importing VPN client settings deletes the existing settings.

To import VPN client settings:

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

STEP 2 Click **Browse** to locate a CSV file containing the VPN client settings.

STEP 3 Click **Import** to load the file.

STEP 4 A warning message appears saying “This operation will replace the existing VPN user settings. Are you sure to continue?” Click **Yes**.

Configuring Basic VPN Setup

The CVR100W supports site-to-site VPN for a single gateway-to-gateway VPN tunnel. In this configuration, the CVR100W creates a secure connection to another VPN-enabled router. For example, you can configure the CVR100W 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 a CVR100W at each remote site to provide secure connectivity.

Viewing Default VPN Settings

The basic VPN setup sets most parameters to defaults as proposed by the VPN Consortium (VPNC), and assumes a pre-shared key, which greatly simplifies the setup.

To view the default VPN settings on your CVR100W:

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

STEP 2 Click **View Default Settings**.

The following default VPN settings are displayed:

Basic VPN Setup Default Values for IKE	
Exchange Mode	Main
Local WAN (Internet) ID	Local WAN (Internet) IP Address
Remote WAN (Internet) ID	Remote WAN (Internet) IP Address
Encryption Algorithm	AES-128
Authentication Algorithm	SHA-1
Authentication Method	Pre-Shared Key

Diffie-Hellman (DH) Group	Group2 (1024 bit)
SA-Lifetime	8 Hours
Basic VPN Setup Default Values for VPN	
Encryption Algorithm	AES-128
Integrity Algorithm	SHA-1
SA-Lifetime	1 Hours
PFS Key Group	DH-Group 2 (1024 bit)

STEP 3 Click **Back** to return to the Basic VPN Setup page.

Configuring Basic VPN Settings

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

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

STEP 2 Enter the following information:

Policy Name and Remote IP Type	
Policy Name	Enter a unique name for the VPN policy. The VPN policy name cannot be same as the username of an existing VPN client.
Pre-Shared Key	Enter the pre-shared key, or password, that will be exchanged between the two routers. It must be between 8 and 49 characters.
Endpoint Information	
Remote Endpoint	Choose the way that the remote endpoint, or the router to which the CVR100W will connect, is identified by IP address or FQDN (Fully-qualified Domain Name).
Remote WAN (Internet) IP Address	Enter the public IP address or domain name of the remote endpoint.

Redundancy Endpoint	Choose the way that the remote redundancy endpoint, or the router to which the CVR100W will connect, is identified by IP address or FQDN.
Redundancy WAN (Internet) IP Address	Enter the public IP address or domain name of the remote redundancy endpoint.
Local WAN (Internet) IP Address	Enter the public IP address or domain name of the local endpoint (CVR100W).
Secure Connection Remote Accessibility	
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 (Local Network) 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 CVR100W.
Local LAN (Local Network) Subnet Mask	Enter the private network (LAN) subnet mask of the local network (CVR100W).

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 are acceptable.

STEP 3 Click **Save**.

STEP 4 Click **Back**. The Advanced VPN Setup page opens. You can configure advanced VPN settings on this page.

Configuring Advanced VPN Setup

The Advanced VPN Setup page allows you to configure advanced VPN parameters, such as IKE and other VPN policies. These policies control how the CVR100W initiates and receives VPN connections with other endpoints.

Configuring Global Advanced VPN Settings

You can globally enable or disable NAT Traversal and NetBIOS on the CVR100W.

To configure NAT Traversal and NetBIOS on your CVR100W:

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

STEP 2 Enter the following information:

- **NAT Traversal:** Check **Enable** to apply the NAT settings for both the local network and the remote network communicating over the VPN tunnel. This option is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.
- **NetBIOS:** Check **Enable** to allow access remote network resources by using its NetBIOS name, for example, browsing Windows Neighborhood. NetBIOS broadcasting can resolve a NetBIOS name to a network address. This option allows NetBIOS broadcasts to travel over the VPN tunnel.

STEP 3 Click **Save**.

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 and encryption algorithms, 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** > **Advanced VPN Setup**.

In the **IKE Policy Table** area, all existing IKE policies used for the VPN policies are displayed.

STEP 2 To create a new IKE policy, click **Add Row**.

Other options: To edit an IKE policy, choose an entry and click **Edit**. To delete an IKE policy, choose an entry and click **Delete**.

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.

STEP 3 Enter the following information:

Policy Name	Enter a unique name for the policy for identification and management purposes. The VPN policy name cannot be same as the username of an existing VPN client.
Exchange Mode	Choose one of the following options: ▪ **Main Mode:** This mode negotiates the tunnel with higher security, but is slower. ▪ **Aggressive Mode:** This mode establishes a faster connection, but with lowered security.
Respondent Mode	Check **Enable** to set the CVR100W to work as a VPN respondent. The CVR100W can only receive the VPN request from remote VPN peer.

Local ID	Choose how to specify your local gateway ID. ▪ Click **Auto** to automatically to obtain the local gateway ID. ▪ Click **Manual** to enter the IP address or the fully qualified domain name (FQDN) of the local gateway ID.
Remote ID	Choose how to specify the remote gateway ID. ▪ Click **Auto** to automatically to obtain the remote gateway ID. ▪ Click **Manual** to enter the IP address or the fully qualified domain name (FQDN) of the remote gateway ID.
Encryption Algorithm	Choose the algorithm used to negotiate the Security Association (SA): DES, 3DES, AES-128, AES-192, or AES-256.
Authentication Algorithm	Specify the authentication algorithm for the VPN header: MD5, SHA-1, or SHA2-256. Ensure that the authentication algorithm is configured identically on both sides of the VPN tunnel (for example, the CVR100W 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 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 (SA) becomes invalid.
Dead Peer Detection	Check **Enable** to enable this feature, or uncheck to disable it. Dead Peer Detection (DPD) detects whether the peer is alive or not. If the peer is detected as dead, the router deletes the IPsec and IKE Security Association.

DPD Delay	If you enable DPD, 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	If you enable DPD, enter the maximum time that the CVR100W should wait to receive a response to the DPD message before considering the peer to be dead.

STEP 4 Click **Save**. Then click **Back** to return to the Advanced VPN Setup page.

Configuring VPN Policies

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

To configure a VPN policy:

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

In the **VPN Policy Table** area, all existing VPN policies used to establish the site-to-site VPN tunnels are displayed.

STEP 2 To create a new VPN policy, click **Add Row**.

Other options: To edit a VPN policy, choose an entry and click **Edit**. To delete a VPN policy, choose an entry and click **Delete**. To enable a VPN policy, choose an entry and click **Enable**. To disable a VPN policy and terminate the corresponding VPN connection (if applicable), choose an entry and click **Disable**.

NOTE If you have a VPN connection already configured, you cannot add another without deleting the existing VPN connection.

STEP 3 Enter the following information:

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 endpoint. 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**. Then enter the identifier in the space provided.
Redundancy Endpoint	Check **Enable** to enable the redundancy gateway feature so that the CVR100W can connect to a backup VPN endpoint when the primary VPN connection fails. If you enable this feature, specify the IP address or FQDN of the remote redundancy endpoint or the router to which the CVR100W will connect when the primary VPN connection fails.
Rollback enable	Check to switch to the primary VPN connection by disabling the backup VPN connection when the primary VPN connection has recovered from a failure. **NOTE** DPD should be enabled if you want to use the Redundant Endpoint feature for IPsec VPN connection.
Local Traffic Selection	
Local IP	Select the type of identifier that you want to provide for the local peer: ▪ **Single:** Limits the policy to one host. Enter the IP address of the local host that will be part of the VPN in **IP Address** field. ▪ **Subnet:** Allows an entire subnet to connect to the VPN. Enter your local network address in the **IP Address** field, and enter the subnet mask in the **Subnet Mask** field.

IP Address	Enter the IP address of the local host if the Local IP is set to Single, or enter your local network address if the Local IP is set to Subnet.
Subnet Mask	Enter the subnet mask, such as 255.255.255.0, if the Local IP is set to Subnet.
Remote Traffic Selection	
Remote IP	Select the type of identifier that you want to provide for the remote peer: ▪ **Single:** Limits the policy to one remote host. Enter the IP address of the remote host that will be part of the VPN in **IP Address** field. ▪ **Subnet:** Allows an entire subnet to connect to the VPN. Enter the remote network address in the **IP Address** field, and enter the subnet mask in the **Subnet Mask** field.
IP Address	Enter the IP address of the remote host if the Remote IP is set to Single, or enter the remote network address if the Remote IP is set to Subnet.
Subnet Mask	Enter the subnet mask, such as 255.255.255.0, if the Remote IP is set to Subnet.
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	
Manual Policy Parameters For a Manual policy type, enter the settings in the **Manual Policy Parameters** area.	
SPI-Incoming	Enter a hexadecimal value between 3 and 8 characters; for example, 0x1234.
SPI-Outgoing	Enter a hexadecimal value between 3 and 8 characters.

Encryption Algorithm	Select the algorithm used to encrypt the data: DES, 3DES, AES-128, AES-192, or 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, or 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.

Auto Policy Parameters

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

SA-Lifetime	Enter the duration of the Security Association (SA) 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 **Enable** to enable Perfect Forward Secrecy (PFS) to improve security. While slower, this protocol helps to prevent intruders 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 CVR100W.

STEP 4 Click **Save**. Then click **Back** to return to the Advanced VPN Setup page.

STEP 5 Click **IPSec Connection Status** to see the status of all site-to-site VPN policies on the CVR100W.

Managing Certificates

The CVR100W 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 CVR100W.

Generating a New Certificate

You can generate a new certificate to replace the existing certificate on the CVR100W.

To generate a certificate:

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

STEP 2 Click the **Generate a New Certificate** radio button.

STEP 3 Click **Generate Certificate**.

Importing Certificates

You can import certificates previously saved to a file.

To import a certificate:

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

STEP 2 Click the **Import Certificate From a File** radio button.

STEP 3 Click **Browse** and locate a 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 CVR100W's configuration is restored to the factory default settings, this certificate can be imported and restored on the CVR100W.

To export a certificate for Admin:

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

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

The certificate for administrator (admin.pem) will be saved to your local PC.

Exporting Certificates for Client

The certificate for client allows the QuickVPN users to securely connect to the CVR100W. The certificate must be placed in the installation directory of the QuickVPN client.

To export a certificate for client:

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

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

The certificate for client (client.pem) will be saved to your local PC.

Configuring VPN Passthrough

VPN Passthrough allows VPN traffic that originates from VPN clients to pass through your CVR100W.

To configure VPN passthrough:

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

STEP 2 Choose the type of traffic to allow to pass through the CVR100W:

IPsec Passthrough	Check **Enable** to allow IP security tunnels to pass through the CVR100W.
PPTP Passthrough	Check **Enable** to allow Point-to-Point Tunneling Protocol (PPTP) tunnels to pass through the CVR100W.
L2TP Passthrough	Check **Enable** to allow Layer 2 Tunneling Protocol (L2TP) tunnels to pass through the CVR100W.

STEP 3 Click **Save**.

7

Configuring Quality of Service (QoS)

This chapter describes how to configure the quality of service (QoS) features. It includes the following sections:

- **Configuring Bandwidth Management**
- **Configuring QoS Port-Based Settings**
- **Configuring CoS Settings**
- **Configuring DSCP Settings**

Configuring Bandwidth Management

You can 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 CVR100W 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**.

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

Upstream	The bandwidth (kbs) used for sending data to the Internet.

Downstream	The bandwidth (kbs) 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 the bandwidth usage.

To configure the bandwidth priorities:

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

STEP 2 In the **Bandwidth Management** field, check **Enable**.

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

STEP 4 Enter the following information:

Enable	Check to enable bandwidth management for this service.
Service Name	Choose the service to prioritize.
Direction	Choose the direction of the traffic that you want to prioritize (**Downstream** or **Upstream**).
Priority	Choose the priority of the service (**Low**, **Normal**, **Medium**, or **High**).

STEP 5 Click **Save**.

STEP 6 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**.

STEP 7 To delete an entry from the table, check the relevant box and click **Delete**. Then, click **Save**.

STEP 8 To add a new service definition, click **Configure Services**. You can define a new service to use for all firewall and QoS definitions. See **Configuring Service Management** for more information.

Configuring QoS Port-Based Settings

You can configure QoS settings for each LAN port on the CVR100W. The CVR100W supports 4 priority queues that allow for traffic prioritization per physical switch port.

To configure QoS settings for the LAN ports:

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

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

Trust Mode	Choose one of the following options from the drop-down menu: ▪ **Port:** 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. ▪ **DSCP:** Differentiated Services Code Point (DSCP). Enabling this feature prioritizes the network traffic across the LAN based on the DSCP queue mapping on the DSCP Settings page. ▪ **CoS:** Class of Service (CoS). Enabling this feature prioritizes the network traffic across the LAN based on the CoS queue mapping on the CoS Settings page.
Default Traffic Forwarding Queue for Untrusted Devices	Choose a priority level for outbound traffic (1 to 4).

STEP 3 Click **Save**.

STEP 4 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 CVR100W.

NOTE You first need to go to the QoS Port-Based Settings page by clicking the link on this page to set the trust mode to CoS.

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**.

STEP 4 To restore the default CoS settings, click **Restore Default**.

Configuring DSCP Settings

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

NOTE You first need to go to the QoS Port-Based Settings page by clicking the link on this page to set the trust mode to DSCP.

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 radio 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**.

STEP 5 To restore the default DSCP settings, click **Restore Default**.

8

Administering Your CVR100W

This chapter describes the administration features of the CVR100W, including user management, network management, system diagnostics and logs, date and time, and other settings. It includes the following sections:

- Configuring Password Complexity
- Configuring Administrator Account Settings
- Configuring Remote Management
- Configuring Port Management
- Configuring Do-Not-Disturb Mode
- Configuring System Time
- Configuring Bonjour
- Using Diagnostic Tools
- Configuring Logging
- Backing Up and Restoring System Configuration
- Upgrading Firmware
- Rebooting the CVR100W
- Restoring the Factory Defaults
- Running the Setup Wizard

Configuring Password Complexity

The CVR100W can enforce the minimum password complexity requirements for password changes.

To configure the password complexity settings:

STEP 1 Choose **Administration** > **Password Complexity**.

STEP 2 In the **Password Complexity Settings** field, check **Enable**.

STEP 3 Configure the following password complexity settings:

- **Minimum Password Length:** Enter the minimum password length (0 to 64 characters). The default is 8 characters.
- **Minimum number of character classes:** Enter a number representing one of the following character classes:
  - Uppercase letters
  - Lowercase letters
  - Numbers
  - Special characters available on a standard keyboard

  By default, passwords must contain characters from at least three of these classes.
- **The new password must be different than the current one:** Check **Enable** to require that new passwords differ from the current password.
- **Password Aging:** Check **Enable** to expire passwords after a specified time.
- **Password aging time:** Enter the number of days after which the password expires (1 to 365). The default is 180 days.

STEP 4 Click **Save**.

Configuring Administrator Account Settings

You can change the username and password for the administrative user (default user name and password: “cisco”).

To edit the settings for the administrative user:

STEP 1 Choose **Administration** > **User**.

STEP 2 To edit the settings for the administrative user, enter the following information:

New Username	Enter a new username.
Old Password	Enter the current password.
New Password	Enter the new password. We recommended that you ensure 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.
Password Strength Meter	Displays the strength of the password that you entered. ▪ **Red:** Password fails to meet the minimum complexity requirements. ▪ **Yellow:** Password meets the minimum requirements but the password strength is weak. ▪ **Green:** Password is strong.

STEP 3 Check **Hide Password** to show the password in ciphertext.

STEP 4 Check **Blank Password** to set the password blank (not recommended).

STEP 5 Check **Disable Password Strength Enforcement** to disable password strength enforcement (nor recommended). Disabling password strength enforcement will increase your network security risk.

STEP 6 Click **Save**.

Configuring Remote Management

You can access web-based Configuration Utility from the LAN side by using the CVR100W's LAN IP address and HTTPS (HTTP over SSL) or HTTP, or from the WAN side by using the CVR100W's WAN IP address and HTTPS or HTTP.

To configure remote management:

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

STEP 2 In the **Web Access** field, select the way that you access web-based Configuration Utility from a local PC.

- **HTTP:** Check to allow you to access web-based Configuration Utility from the LAN side by using the CVR100W's LAN IP address and HTTP.
- **HTTPS:** Check to allow you to access web-based Configuration Utility from the LAN side by using the CVR100W's LAN IP address and HTTPS.

STEP 3 In the **Remote Management** field, check **Enable** to enable remote management. Enabling this feature allows you to remotely manage the CVR100W from the WAN side by using the CVR100W's WAN IP address.

STEP 4 In the **Remote Access** field, select the way that you access web-based Configuration Utility from a remote WAN network.

- **HTTP:** Check to allow you to access web-based Configuration Utility from a remote WAN network by using the CVR100W's WAN IP address and HTTP.
- **HTTPS:** Check to allow you to access web-based Configuration Utility from a remote WAN network by using the CVR100W's WAN IP address and HTTPS.

STEP 5 In the **Remote Upgrade** field, check **Enable** to allow you to upgrade the firmware remotely.

STEP 6 In the **Allowed Remote IP Address** field, click the **Any IP Address** radio button to allow any IP address from a remote WAN network to access the CVR100W, or enter a range of IP addresses in the address fields to restrict remote access to the hosts in the specified remote network.

STEP 7 In the **Remote Management Port** field, enter the port number for remote management. The default value is 8080.

STEP 8 Click **Save**.

Configuring Port Management

Use the Port Management page to configure the duplex mode and speed for the physical ports and control the flow on the ports.

To configure port management:

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

The following information is displayed:

- **Port:** Displays the port type and port identification.
- **Link:** Shows if the link through the port is up or down.
- **Mode:** Displays the current duplex mode and speed.
- **Flow Control:** Shows if flow control is enabled or disabled on the port.

STEP 2 To configure the duplex mode and speed of a port, choose an option from the **Mode** drop-down menu. The available options are:

- **Auto Negotiation:** Lets the system and network determine the optimal port speed.
- **10 Mbps Half Duplex or 100 Mbps Half Duplex:** The 10/100 Mbps port supports transmissions between the device and the client in only one direction at a time.
- **10 Mbps Full Duplex or 100 Mbps Full Duplex:** The 10/100 Mbps port supports transmissions between the device and the client in both directions simultaneously.

STEP 3 To control the flow on a port, check the **Flow Control** box on that port.

STEP 4 Click **Save**.

Configuring Do-Not-Disturb Mode

The Do-Not-Disturb Mode feature turns on or turns off all lights of the CVR100W. You can enable this feature by pressing the Do-Not-Disturb Mode button on the front panel or from web-based Configuration Utility.

NOTE Enabling this feature will not affect the normal operation of the CVR100W.

To enable the Do-Not-Disturb mode from web-based Configuration Utility:

STEP 1 Choose **Administration** > **Do-Not-Disturb Mode**.

STEP 2 Check **Enable** to enable the Do-Not-Disturb mode on the CVR100W.

STEP 3 Click **Save**.

Configuring System Time

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 CVR100W 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 Specify the time zone from the **Time zone** drop-down menu.

STEP 3 In the **Adjust for Daylight Savings Time** field, check the box to adjust the time for Daylight Savings Time.

STEP 4 In the **Set Date and Time** field, choose how to set the date and time.

- **Auto:** Click this radio button to automatically synchronize the date and time with the specified NTP server.
- **Manual:** Click this radio button to manually set the date and time.

STEP 5 If you choose **Auto** to set the system time, enter the following information in the **NTP Server** fields:

- To use the default NTP servers, click the **Use Default** radio button.

- To use a specific NTP server, click the **User Defined NTP Server** radio button and enter the fully-qualified domain name (FQDN) or IP address of the NTP servers in the two available fields.

STEP 6 If you choose **Manual** to set the system time, enter the date and time in the **Manually Set System Time** fields.

STEP 7 Click **Save**.

Configuring Bonjour

Bonjour is a service advertisement and discovery protocol. On the CVR100W, it 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**.

Using Diagnostic Tools

The CVR100W provides several diagnostic tools to help you troubleshoot network problems.

Network Tools

Using Ping/Traceroute

You can use the Ping tool to test connectivity between the CVR100W and another device in the network or to test connectivity to the Internet by pinging a fully qualified domain name (for example, 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's IP address or a fully qualified domain name (FQDN) such as 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 and return to the Network Tools page.

Using Traceroute

The Traceroute utility displays all the routers present between the destination IP address and the CVR100W.

To use Traceroute:

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

STEP 2 In the **IP Address / Domain Name** field, enter the IP address or a fully qualified domain name (FQDN) such as www.cisco.com to trace.

STEP 3 Click **Traceroute**.

The Traceroute results appear.

STEP 4 Click **Close** when done and return to the Network Tools page.

Performing a DNS Lookup

You can use the Lookup utility 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 **Look up**. If the host or domain entry exists, you will see a response with the IP address.

To use the Lookup utility:

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

STEP 2 In the **Internet Name** field, enter the Internet name of the host.

STEP 3 Click **Look up**.

The nslookup results appear.

STEP 4 Click **Close** when done and return to the Network Tools page.

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.

To configure port mirroring:

STEP 1 Choose **Administration** > **Diagnostics** > **Port Mirroring**.

STEP 2 In the **Mirror Source** area, check the ports to mirror.

STEP 3 In the **Mirror Port** area, choose a mirror port.

STEP 4 Click **Save**.

Configuring Logging

The Logging page allows you to configure the logging settings on the CVR100W.

Configuring Logging Settings

To configure the logging settings:

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

STEP 2 In the **Log Mode** field, check **Enable** to enable the logging feature.

STEP 3 In the **Log Severity for Local Log** field, check the log severities for the events that you want to log:

For example: If you check Critical, all log messages listed under the Critical, Emergency, and Alert categories are saved to the local syslog daemon.

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.
Information	Device information.
Debugging	Provides detailed information about an event.

STEP 4 Click **Save**.

Configuring Remote Syslog Server

To configure the remoter syslog server and specify which severity levels of the logs are saved:

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

STEP 2 In the **Log Mode** field, check **Enable** to enable the logging feature.

STEP 3 In the **Remote Log Server** table, click **Add Row**.

STEP 4 In the **Remote Log Server** field, enter the IP address of the remote syslog server.

STEP 5 In the **Log Severity** field, check which severity of events to log.

STEP 6 In the **Enable** field, check the box to enable the remote syslog server.

STEP 7 Click **Save**.

STEP 8 To delete an entry in the Remote Log Server table, select the entry and click **Delete**. To edit an entry in the Remote Log Server table, select the entry and click **Edit**. Make your changes, then click **Save**.

Backing Up and Restoring System Configuration

You can back up custom configuration for later restoration or restore the system configuration from a previous backup from the **Administration** > **Backup / Restore Settings** page.

CAUTION During a restore operation, do not try to go online, turn off the CVR100W, shut down the PC, or use the CVR100W until the operation is complete. This should take about a minute.

Backing Up Your Current Configuration

You can back up your current settings as a configuration file to your local PC. You should always back up your configuration whenever you make any modifications to the device configuration or performing any firmware updates.

To back up your current system configuration:

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

STEP 2 Click **Backup Configuration**.

Restoring Your Configuration from a Saved Configuration File

You can restore the system configuration from a previously-saved configuration file.

To restore the settings from a saved configuration file on your local PC:

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

STEP 2 Click **Browse** to locate the configuration file.

STEP 3 Select the file and click **Browse**.

STEP 4 Click **Restore Configuration**.

The CVR100W uploads the configuration file and uses its settings to update the system configuration. Then the CVR100W restarts and uses the new configuration.

Upgrading Firmware

You can upgrade the CVR100W to a newer firmware from the **Administration** > **Firmware 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.

To upgrade to a newer version of the firmware:

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

The following information is displayed:

- **Device Model:** Displays the device model.
- **PID VID:** Displays the product ID and version ID.
- **Current Firmware Version:** Displays the firmware version that the CVR100W is currently using.

STEP 2 In the **Download the latest firmware** field, click **Download** to download the latest version of the firmware from the specified website to your local PC. Make sure that you have an active WAN connection.

STEP 3 In the **Locate & select the upgrade file** field, click **Browse** to locate and select the downloaded firmware image from your local PC.

STEP 4 Click **Start Upgrade**.

After the new firmware image is validated, the new image is written to flash, and the CVR100W is automatically rebooted with the new firmware.

CAUTION Resetting the CVR100W to its default factory settings erases all of your custom settings.

STEP 5 Go to the **Status** > **System Summary** page to make sure that the CVR100W is using the new firmware version.

Rebooting the CVR100W

To reboot the CVR100W, you can press and release the **RESET** button on the back panel for less than 5 seconds, or perform the **Reboot** operation from web-based Configuration Utility.

To reboot the CVR100W from web-based Configuration Utility:

STEP 1 Choose **Administration** > **Reboot**.

STEP 2 Click **Reboot**.

Rebooting the device will close all current sessions and the system will be down for several seconds.

Restoring the Factory Defaults

To restore the CVR100W to the factory default settings, you can press and hold the **RESET** button on the back panel for more than 5 seconds, or perform the **Reset to Factory Defaults** operation from web-based Configuration Utility.

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.

NOTE The Reset To Factory Defaults operation will wipe out the current settings used on the CVR100W. We recommend that you back up your current settings before restoring the CVR100W to the factory default settings.

To restore the CVR100W to its factory default settings:

STEP 1 Choose **Administration** > **Restore Factory Defaults**.

STEP 2 Click **Restore Factory Defaults**.

This reboots the unit and restores the CVR100W to the factory default settings. The settings that you have previously made to the CVR100W are lost.

Running the Setup Wizard

You can use the Setup Wizard to quickly configure the initial settings of your CVR100W.

To launch the Setup Wizard and complete the initial configuration:

STEP 1 Choose **Administration** > **Setup Wizard**.

The Configure Admin Password page opens. From this page you can enter a new administrative password.

The administrative password protects your CVR100W from unauthorized access. For security reasons, you should change the password from its default setting. Write this password down for future reference. A blank password is not recommended.

- **Router Password:** Enter a new password. Passwords should not contain dictionary words from any language. They should contain a mixture of letters (both uppercase and lowercase), numbers, and symbols. Passwords must be at least 8 but no more than 64 characters in length.
- **Hide Password**: Check to show the password in ciphertext.
- **Blank Password**: Check to set the password blank (not recommended). This option is only available when you disable password strength enforcement.
- **Password Strength Meter:** Displays the strength of the password that you entered.
  - **Red:** Password fails to meet the minimum complexity requirements.
  - **Yellow:** Password meets minimum the requirements but the password strength is weak.

- **Green:** Password is strong.

- **Disable Password Strength Enforcement:** Check to disable password strength enforcement (nor recommended). Disabling password strength enforcement will increase your network security risk.

STEP 2 Click **Next** to continue.

The Configure Connection Type page opens. From this page you can select the Internet connection type to connect to the Internet. Call your Internet Service Provider (ISP) if you are not sure what the correct type is.

Specify the corresponding settings based on the selected Internet connection type.

- **DHCP:** This is the default Internet connection type and is often used with cable modems. Choose this option if your ISP dynamically assigns an IP address on connection.

- **PPPoE:** PPPoE uses Point to Point Protocol over Ethernet (PPPoE) to connect to the Internet. Choose this option if your ISP provides you with client software, username, and password. Use the necessary PPPoE information from your ISP to complete the PPPoE configuration.

  - **Account Name:** Enter your username assigned to you by the ISP.

  - **Password:** Enter your password assigned to you by the ISP.

  - **Hide Password:** Check to show the password in ciphertext.

- **Static IP:** Choose this option if the ISP provides you with a static (permanent) IP address and does not assign it dynamically. Use the corresponding information from your ISP to complete the configuration.

  - **Static IP Address:** Enter the IP address of the WAN port.

  - **Subnet Mask:** Enter subnet mask of the WAN port.

  - **Gateway IP:** Enter the IP address of the default gateway.

  - **Primary DNS:** Enter the IP address of the primary DNS server.

  - **Secondary DNS:** (Optional) Enter the IP address of the secondary DNS server.

STEP 3 Click **Next** to continue.

The Configure Wireless Security page opens. From this page you can set the name for your wireless network and select the type of wireless security.

- **Network Name:** Enter a unique name for the wireless network.
- **Security Mode:** Select the type of wireless security and specify the corresponding security settings. We recommend that you use the highest level of security that is supported by the devices in your network. See **Configuring Wireless Security** for more information on configure the wireless security settings.

STEP 4 Click **Next** to continue.

The Confirm Setup Wizard Configuration page opens. From this page you can see the summary information for all configuration.

STEP 5 If the configuration is correct, click **Save and Exit** to complete the configuration. If you click **Exit**, the changes that you made will be lost.

NOTE The Change Password window appears if you exit the Setup Wizard without saving any settings. See **Changing the Default Administrative Password** for more information.

9

Using Cisco Simple Connect

This chapter describes how to configure Cisco Simple Connect and includes the following sections:

- **About Cisco Simple Connect**
- **Configuring Cisco Simple Connect**
- **Connecting to CSC Wireless Network**
- **Customizing Your QR Code**

About Cisco Simple Connect

Cisco Simple Connect (CSC) provides a safe and convenient way for CSC-enabled devices to connect with a Wi-Fi access point by touching the RFiD or scanning the QR code of the CSC card. Cisco Simple Connect makes accessing wireless access points simple and allows you to expand more business applications. See www.cisco.com/go/cn/cvr100w for more information.

By default, Cisco Simple Connect is disabled on the CVR100W. You can set one of the SSIDs (SSID1, SSID2, or SSID3) as the CSC wireless access point. The wireless clients that are associated with the CSC wireless access point can only access the Internet through the CVR100W.

When configuring Cisco Simple Connect, note the following:

- Only SSID1, SSID2, or SSID3 can be set as the CSC wireless access point.
- Enabling Cisco Simple Connect on a SSID does not affect the normal operation of other SSIDs.
- SSID1 must be set as the CSC wireless access point when WDS is enabled on the CVR100W.

- The VLAN to which the CSC wireless access point is mapped cannot be the same as the VLANs of other SSIDs. You must assign a different VLAN to the CSC wireless access point.
- When enabling Cisco Simple Connect on a SSID, the current settings of this SSID are automatically saved before the CSC settings are applied, and then are restored after CSC is disabled on this SSID.
- When disabling Cisco Simple Connect on a SSID, the CSC settings on this SSID are automatically saved before the previous saved settings of this SSID are restored, and are restored after CSC is enabled again.
- By default, the CSC wireless access point is automatically named as Cisco-Simple-Connect after you enable Cisco Simple Connect for the first time. The wireless security mode, SSID broadcast, and SSID Isolation are disabled on the CSC wireless access point. For security purposes, we strongly recommend that you configure the CSC wireless access point with the highest level of security that is supported by the devices into your wireless network.
- The wireless clients that are associated with the CSC wireless access point can only access the Internet. They cannot manage and configure the CVR100W through web-based Configuration Utility and access the CVR100W's local network resources.
- The CVR100W provides you with a unique token key and displays the time that you can access the Internet after you run the CSC client application on a smart phone or panel computer that supports the Android or iOS operating system to interact with the CSC card. The token key is used for the smart devices that do not support the Android or iOS operating system or do not install the CSC client application or the PCs or laptops to access the Internet after they are associated with the CSC wireless network.
- The administrator can limit the time to access the Internet for all wireless clients that are associated with the CSC wireless network. When the online time of the CSC wireless client exceeds the limitation, the wireless connection is automatically terminated.

Configuring Cisco Simple Connect

To enable Cisco Simple Connect and configure the settings of the CSC wireless access point:

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

STEP 2 In the **Wireless Table**, check the SSID that you want to configure and click **Edit**.

STEP 3 Check the **Enable SSID** box to enable this SSID.

STEP 4 Check the **CSC** box to enable Cisco Simple Connect on this SSID.

STEP 5 Select a VLAN from the **VLAN** drop-down menu to which all traffic from the CSC wireless network is mapped. The VLAN that is associated with the CSC wireless network cannot be the same as the VLANs of other SSIDs.

STEP 6 (Optional) Configure the following settings for this SSID:

- **SSID Name:** Enter a unique name for the CSC wireless access point. By default, the name of the CSC wireless access point is set to Cisco-Simple-Connect after you enable Cisco Simple Connect for the first time.

  Generally, you can enter the SSID name that is provided on your CSC card in this field. If you want to customize the name of the CSC wireless access point, enter a new SSID name in this field.

  NOTE When you customize a new name of the CSC wireless access point, you are asked to regenerate and print the QR code of the CSC card. See **Customizing Your QR Code** for more information.

- **Security Mode:** By default, the security mode of the CSC wireless access point is disabled. You can modify its security settings by clicking **Edit Security Mode**. For security purposes, we strongly recommend that you configure the CSC wireless access point with the highest level of security that is supported by the devices into your wireless network.

  Generally, you can choose WPA or WPA2 as the security mode and enter the security key that is provided on your CSC card. If you want to customize the security key of the CSC wireless access point, enter a new security key. See **Configuring Wireless Security** for more information.

  NOTE When you customize a new security key of the CSC wireless access point, you are asked to regenerate and print the QR code of the CSC card. See **Customizing Your QR Code** for more information.

- **MAC Filter:** By default, MAC address filtering is disabled on the CSC wireless access point. You can enable this feature and configure the corresponding settings by clicking **Edit MAC Filter**. See **Configuring MAC Address Filtering** for more information.
- **Time of Day Access:** By default, Time of Day Access is disabled on the CSC wireless access point. You can enable this feature and configure the corresponding settings by clicking **Time of Day Access**. See **Configuring Time of Day Access** for more information.
- **SSID Broadcast, WMM, and SSID Isolation:** By default, these features are enabled on the CSC wireless access point. See **Configuring Wireless Network Settings** for more information.

STEP 7 Click **Save**.

STEP 8 Click **Edit CSC** to limit the time to access the Internet for all wireless clients that are associated with the CSC wireless network.

STEP 9 Enter the following information:

SSID Name	Displays the current name of the CSC wireless access point. By default, it is named as Cisco-Simple-Connect after Cisco Simple Connect is enabled on this SSID for the first time.
Security Mode	Displays the current wireless security mode used on the CSC wireless access point. By default, the security mode is disabled on the CSC wireless access point.
Security Key	Displays the current security key of the CSC wireless access point.
Show Password	Check to show the password in plaintext.
Access Network Time	Enter a value from 0 to 1440 seconds. The default value is 0, which means that there is no limit.

STEP 10 Click **Save**.

Connecting to CSC Wireless Network

If you have a smart device (such as a smart phone or a panel computer) that supports the Google Android or Apple iOS operating system, you can first install the CSC client application on your device and interact with the CSC card (by touching the RFiD or scanning the QR code of the CSC card). Then you are automatically connected to the specified CSC wireless network and are allowed to access the Internet.

To connect to the CSC wireless network:

STEP 1 Download and install the CSC client application on your smart device by using one of the following methods:

- Download the CSC client application to your local PC from Cisco.com (go to www.cisco.com/go/cn/cvr100w, open the **Cisco Simple Connect** tab, and click the download link, and then install it on your device.

  –Or–

- Connect your device to the CSC wireless network (You must first know the SSID name and password of the CSC wireless network), and then open the web browser on your device to try to access a website. The Cisco Simple Connect Hotspot opens. Click the corresponding link to download and install the CSC client application on your device.

STEP 2 Run the CSC client application on your device.

STEP 3 Touch the RFiD or scan the QR code of the CSC card.

You are now automatically connected to the specified CSC wireless network and are allowed to access the Internet. The CVR100W provides you with a unique token key and displays the time that you can access the Internet.

If the CVR100W limits the time to access the Internet, the wireless connection will be terminated until the next legal login when your online time exceeds the limitation.

Customizing Your QR Code

Generally, the CSC card provides you with a unique SSID name and security key for configuring the CSC wireless network, and prints the QR code for scanning by CSC-enabled devices.

This section describes how to customize the SSID name and security key of the CSC wireless network, and then print a new QR code from the CVR100W Resources page.

CAUTION After you customize the SSID name and/or security key other than the default settings that are provided on the CSC card, the CSC card will be invalid. You must reconfigure the CSC wireless network of the CVR100W using the new SSID name and/or security key. The wireless clients need to rescan the new QR code that you print from the CVR100W Resources page to connect to the CSC wireless network.

STEP 1 Launch your web browser and access the CVR100W Resources page:

http://www.cisco.com/go/cn/cvr100w

STEP 2 Click the **Cisco Simple Connect** (思科锐联) tab.

STEP 3 In the **Customize QR Code** (定制二维码) area, enter the following information:

- **Wireless Security** (连接类型)**:** Displays the wireless security mode of the CSC wireless network.
- **SSID Name:** If needed, enter a new SSID name for the CSC wireless network.
- **Security Key** (密码)**:** If needed, enter a new security key for the CSC wireless network.

STEP 4 Click **Generate** (生成). A new QR code that includes the new SSID name and security key of the CSC wireless network is generated.

STEP 5 Click **Print** (打印) to print the new QR code.

STEP 6 Use the new SSID name and security key to reconfigure the CSC wireless network of the CVR100W. See **Configuring Cisco Simple Connect** for more information.

The wireless clients can now use the CSC client application on their CSC-enabled devices to interact with the new QR code and connect to the CSC wireless network.

A

Using Cisco QuickVPN

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

This appendix includes the following sections:

- **Before You Begin**
- **Installing the Cisco QuickVPN Software**
- **Using the Cisco QuickVPN Software**

Before You Begin

The QuickVPN program only works with the CVR100W that is properly configured to accept a QuickVPN connection.

You must perform the following steps:

STEP 1 Enable remote management. See **Configuring Remote Management** for complete details.

STEP 2 Create QuickVPN user accounts. See **Configuring VPN Clients** for complete details.

After a user account is created, the credentials can be used by the QuickVPN client.

Installing the Cisco QuickVPN Software

To download and install the Cisco QuickVPN software:

STEP 1 Go to the **Customer Support Central** link: www.cisco.com/support.

STEP 2 Enter **QuickVPN** in the search box in the **Downloads** tab and find the QuickVPN software.

STEP 3 Save the zip file to your PC, and extract the zip file.

STEP 4 Double-click the .exe file, and follow the on-screen instructions to install the Cisco QuickVPN software.

Using the Cisco QuickVPN Software

To launch the Cisco QuickVPN software and establish the VPN connection with a remote VPN server:

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 username and password that were created in **Configuring VPN Clients**.

STEP 4 In the **Server Address** field, enter the IP address or domain name of the CVR100W.

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**.

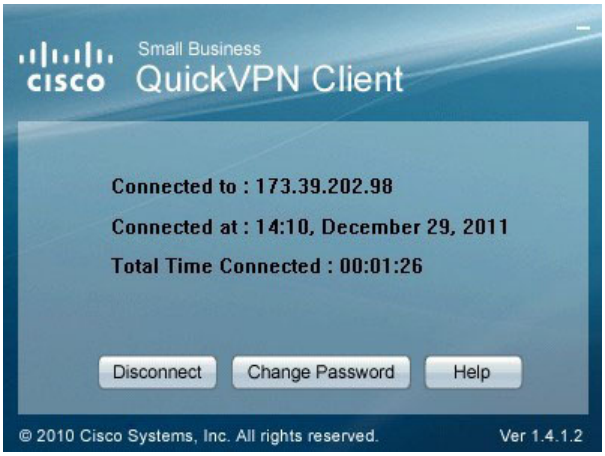
NOTE If there are multiple sites to which you need to create a tunnel, you can create multiple profiles, but only one tunnel can be active at a time.

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 **Configuring VPN Clients** for complete details.

B

Where to Go From Here

Cisco provides a wide range of resources to help you obtain the full benefits of the Cisco CVR100W Wireless-N VPN Router.

Support	
Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport
Cisco Small Business Support and Resources	www.cisco.com/go/smallbizhelp
Phone Support Contacts	www.cisco.com/go/sbsc
Cisco Small Business Firmware Downloads	www.cisco.com/go/smallbizfirmware Select a link to download firmware for Cisco Small Business Products. No login is required.
Product Documentation	
Cisco CVR100W	www.cisco.com/go/cvr100w
Cisco Small Business	
Cisco Partner Central for Small Business (Partner Login Required)	www.cisco.com/web/partners/sell/smb
Cisco Small Business Home	www.cisco.com/smb