ADMINISTRATION GUIDE

Cisco RV215W Wireless-N VPN Firewall

Revised Sep 2014

Contents

4

Getting Started

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

This page appears every time you start Device Manager. To change this behavior, check **Don't show on start up**.

Initial Settings

Change Default Administrator Password	Displays the **Users** page where you can change the administrator password and set up a guest account. See **Configuring User Accounts**.
Launch Setup Wizard	Launches the Setup Wizard. Follow the on-screen instructions.
Configure WAN Settings	Opens the **Internet Setup** page to change parameters such as the router host name. See **Configuring the WAN Settings**.
Configure LAN Settings	Opens the **LAN Configuration** page to modify the LAN parameters, such as the management IP address. See **Configuring the LAN Settings**.
Configure Wireless Settings	Open the **Basic Settings** page to manage the radio. See **Configuring the Wireless Network**.

Quick Access

Upgrade Router Firmware	Open the **Firmware/Language Upgrade** page to update the router firmware or language pack. See **Upgrading Firmware or Changing the Language**.
Add VPN Clients	Opens the **VPN Clients** page to manage virtual private networks. See **VPN Clients**.
Configure Remote Management Access	Opens the **Basic Settings** page to enable the basic features of the router. See **Configuring Basic Firewall Settings**.

Device Status

System Summary	Displays the **System Summary** page that shows the state of the router. See **Viewing the System Summary**.
Wireless Status	Displays the **Wireless Statistics** page that shows the state of the radio. See **Viewing Wireless Statistics**.
VPN Status	Displays the **VPN Status** page that lists the VPN managed by this router. See **Viewing the VPN Status**.

Other Resources

Support	Click to open the Cisco support page.
Forums	Click to visit Cisco online support forums.

Saving Changes

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

Connecting to Your Wireless Network

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

The following steps are provided as an example; it might be necessary to configure client device differently. For instructions that are specific to the client device, consult the device documentation.

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

Your computer might have special software installed to manage wireless connections, or you might find the 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 Setup Wizard.

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

5

Viewing the Status

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

-

Viewing the Dashboard

The **Dashboard** page provides important router information.

To view the Dashboard, choose **Status** > **Dashboard**.

To change the refresh rate of the statistics and parameter values displayed, select the frequency from the **Refresh Rate** drop-down menu.

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

The back panel view shows you the ports that are connected to a device (lit green).

- To view a port connection information, mouse-over the port.
- To refresh the port information, click **Refresh**.
- To close the port information window, click **Close**.

The **Dashboard** page displays the following:

Device Information

- **System Name—**Name of the device.
- **Firmware Version—**Firmware version the device is currently running.
- **Serial Number—**Serial number of the device.

Resource Utilization

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

Syslog Summary

Indicates whether logging is enabled for these event categories:

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

To view the logs, click **details**. For more information see **Viewing Logs**.

To manage logs, click **manage logging**. For more information, see **Configuring Logging Settings**.

LAN (Local Network) Interface

- **MAC Address—**The MAC address of the device.
- **IPv4 Address—**Management IP address of the device.
- **IPv6 Address**—Management IP address of the device (when IPv6 is enabled).
- **DHCP Server—**Status of the device IPv4 DHCP server (enabled or disabled).
- **DHCPv6 Server—**Status of the router IPv6 DHCP server (enabled or disabled).

To view the LAN settings, click **details**. For more information, see **Configuring the LAN Settings**.

WAN (Mobile Network) Information

- **IPv4 Address**—IPv4 address of the USB port.
- **State**—State of the mobile network WAN connection (up or down).

To view the WAN settings, click details. For more information see **Configuring the Wired WAN Connections**.

WAN (Internet) Information

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

To view the WAN settings, click **details**. For more information see **Configuring the Wired WAN Connections**.

Wireless Networks

Lists the status of the four wireless network SSIDs.

To view the router wireless settings, click **details**. For more information see **Viewing Wireless Statistics**.

VPN

QuickVPN Users—Number of QuickVPN users.

PPTP—Number of Point-to-Point Tunneling Protocol (PPTP) users.

Viewing the System Summary

The **System Summary** page displays a summary of the device values, such as the firmware version and serial number.

To view a summary of system settings, choose **Status** > **System Summary**.

To go to the related window, click the underscored parameter. For example, to modify the LAN IP address, click **LAN IP**. The LAN Configuration window appears.

Click **Refresh** to obtain the latest information.

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

System Information

- **Firmware Version—**Current software version the device is running.
- **Firmware MD5 Checksum—**The message-digest algorithm used to verify the integrity of files.

- **Locale**—The language installed on the router.
- **Language Version**—The version of the installed language pack. The language pack version should be compatible with the currently installed firmware. In some cases, an older language pack may be used with a newer firmware image. The router will check the language pack version to see if it is compatible with the current firmware version.
- **Language MD5 Checksum**—The MD5 checksum of the language pack.
- **CPU Model—**Chipset of CPU currently used.
- **Serial Number—**Serial number of the device.
- **System Up Time—**How long the system has been running.
- **Current Time—**Time of day.
- **PID VID—**Product ID and version ID of the device.

IPv4 Configuration

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

IPv6 Configuration

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

- **DNS 1—**IP address of the primary DNS server.
- **DNS 2—**IP address of the secondary DNS server.

Wireless Summary

- **SSID 1—**Public name of the first wireless network.
  - **Security—**Security setting for SSID 1.
- **SSID 2—**Public name of the second wireless network.
  - **Security—**Security setting for SSID 2.
- **SSID 3—**Public name of the third wireless network.
  - **Security—**Security setting for SSID 3.
- **SSID 4—**Public name of the fourth wireless network.
  - **Security—**Security setting for SSID 4.

Firewall Setting Status

- **DoS (Denial of Service)—**Indicates whether DoS prevention is on or off.
- **Block WAN Request—**Indicates whether WAN request blocking is on or off.
- **Remote Management—**Indicates whether or not Device Manager can be accessed remotely.

VPN Setting Status

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

Viewing Wireless Statistics

The **Wireless Statistics** page shows wireless statistics for the device radio.

To view wireless statistics, choose **Status** > **Wireless Statistics**.

To change the refresh rate, choose a refresh rate from the **Refresh Rate** drop-down menu.

To show the bytes in kilobytes (KB) and the numerical data in rounded-up values, check **Show Simplified Statistic Data** and click **Save**. By default, byte data is displayed in bytes and other numerical data is displayed in long form.

To reset the wireless statistics counters, click **Clear Count**. Also the counters are reset when the device is rebooted.

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

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

Viewing the VPN Status

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

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

The **VPN** page displays this information:

Username	The username of the VPN user associated with the QuickVPN PPTP tunnel.
Remote IP	Displays the IP address of the remote QuickVPN client. This could be a NAT/Public IP if the client is behind the NAT router.
Status	Displays the current status of the 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 when the VPN user established a connection.
End Time	Time when the VPN user ended a connection.
Duration (Seconds)	Duration of time between the VPN user establishing and ending a connection.
Protocol	Protocol that the user uses.

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

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

Viewing the IPSec Connection Status

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

STEP 1 Choose **Status** > **IPSec Connection Status**. The table displays the following information:

- **Refresh Rate**—Choose the rate at which you want the data display to clear and display the newest data.
- **Show Simplified Statistic Data**—By default, byte data is displayed in bytes and other numerical data is displayed in long form. To show the bytes in kilobytes (KB) and the numerical data in rounded-up form, check **Show Simplified Statistic Data**.
- **Policy Name**—Name of the VPN policy for which data is displayed.
- **Local or Remote**—Displays the local and remote IP addresses.
- **Start Time and End Time**—Displays the start and end times of the IPsec connections.
- **Duration**—Displays the elapsed time for which the connection is or was active.
- **Packet**—Displays the received (Rx) and transmitted (Tx) packets on the connection.
- **Byte**—Displays the received (Rx) and transmitted (Tx) bytes on the connection.
- **State**—Displays the state of the connection (for example, active or not connected).
- **Action**—Displays actions you can perform on the connection (for example, disconnect).
- **Ext Action**—Displays if you can switch between the primary and the secondary VPN connections. If the **Rollback enable** check box on the **Advanced VPN Parameters** page is checked, the **Switch** button is dimmed.

STEP 2 If you made any changes, click **Save**.

Viewing Logs

The **View Logs** page displays the device logs.

To view the logs, choose **Status** > **View Logs**.

To display the latest log entries, click **Refresh Logs**.

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

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

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

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

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

To save log messages to an external USB device, click **Save Log to USB**.

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

Use the page navigation buttons to move between log pages.

Viewing Connected Devices

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

The IPv4 ARP Table displays information from devices that have responded to the Address Resolution Protocol (ARP) request. If a device does not respond to the request, it is removed from the list.

The IPv6 NDP Table displays all IPv6 Neighbor Discover Protocol (NDP) devices connected to the local link.

To view connected devices, choose **Status** > **Connected Devices**.

To specify the types of interfaces to display, select a value from the **Filter** drop-down menu:

All—All devices connected to the router.

Wireless—All devices connected through the wireless interface.

Wired—All devices connected through the Ethernet ports on the router.

WDS—All Wireless Distribution System (WDS) device connected to the router.

Viewing Port Statistics

The **Port Statistics** page displays port detailed activity.

To view port statistics, choose **Status** > **Port Statistics**.

To cause the page to re-read the statistics from the router and refresh the page, choose a refresh rate from the **Refresh Rate** drop-down menu.

To show the bytes in kilobytes (KB) and the numerical data in rounded-up form, check **Show Simplified Statistic Data** and click **Save**. By default, byte data is displayed in bytes and other numerical data is displayed in long form.

To reset the port statistics counters, click **Clear Count**.

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

Interface	Name of the network interface.
Packet	Number of received/sent packets.
Byte	Number of received/sent bytes of information per second.
Error	Number of received/sent packet errors.
Dropped	Number of received/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 the Guest Network Status

The guest network statistics displays information about the wireless guest network configured on the device.

To view the guest network status, choose **Status** > **GuestNet Status**. The following information is displayed:

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

Viewing the Mobile Network Status

The mobile network statistics about the mobile 3G/4G network and communication device (dongle) configured on the device.

To view the mobile network status, choose **Status** > **Mobile Network**. The following information is displayed:

- **Connection**—Device connected to the guest network.
- **Internet IP Address**—IP address assigned to the USB device.
- **Subnet Mask**—Subnet mask of the USB device.
- **Default Gateway**—IP address of the default gateway.
- **Connection Up Time**—How long the link has been up.
- **Current Session Usage**—Volume of data being received (Rx) and transmitted (Tx) on the mobile link.
- **Manufacturer**—Card manufacturer name.
- **Card Model**—Card model number.
- **Card Firmware**—Card firmware version.
- **SIM Status**—Subscriber identification module (SIM) status.
- **IMS**—The unique identification associated with the GSM, UMTS, or LTE network mobile phone users.
- **Carrier**—Mobile network carrier.
- **Service Type**—Type of service accessed.
- **Signal Strength**—Strength of the wireless mobile network signal.

6

Configuring Networking

This chapter describes how to configure the device network settings.

-

Configuring the Wired WAN Connections

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

Configuring DHCP (Automatic Configuration)

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

To configure the DHCP WAN settings:

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

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

STEP 3 Click **Save**.

Configuring Static IP

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

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

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

STEP 3 Enter this information:

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

STEP 4 Click **Save**.

Configuring PPPoE

To configure the Point-to-Point Protocol over Ethernet (PPPoE) settings:

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

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

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

Username	The username assigned by the ISP.
Password	The password assigned 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. In the redial period field, enter the number of seconds after which the device attempts to reconnect if it is disconnected.

Authentication Type	**Auto-negotiation**—The server sends a configuration request specifying the security algorithm set on it. The device then sends back authentication credentials with the security type sent by the server. **PAP**—Password Authentication Protocol (PAP), used by Point-to-Point Protocol to connect to the ISP. **CHAP**—Challenge Handshake Authentication Protocol (CHAP) requires that both the client and server know the plaintext of the secret to use ISP services. **MS-CHAP or MS-CHAPv2**—The Microsoft version of CHAP, used to access ISP services.

STEP 4 Click **Save**.

Configuring PPTP

To configure the PPTP settings:

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

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

STEP 3 Enter this information:

Internet IP Address	IP address of the WAN port.
Subnet mask	Subnet mask of the WAN port.
Default Gateway	IP address of the default gateway.
PPTP Server	IP address of the Point-To-Point Tunneling Protocol (PPTP) server.
Username	The username assigned to you by the ISP.
Password	The 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. In the redial period field, enter the number of seconds after which the device attempts to reconnect if it is disconnected.
Authentication Type	Choose the authentication type: **Auto-negotiation**—The server sends a configuration request specifying the security algorithm set on it. The device then sends back authentication credentials with the security type sent earlier by the server. **PAP**—The device uses the Password Authentication Protocol (PAP) to connect to the ISP. **CHAP**—The device uses the Challenge Handshake Authentication Protocol (CHAP) when connecting with the ISP. **MS-CHAP or MS-CHAPv2**—The device uses Microsoft Challenge Handshake Authentication Protocol when connecting with the ISP.

STEP 4 Click **Save**.

Configuring L2TP

To configure the L2TP settings:

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

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

STEP 3 Enter this information:

Internet IP Address	Enter the IP address of the WAN port.
Subnet mask	Enter the subnet mask of the WAN port.
Default Gateway	Enter the IP address of the default gateway.
L2TP Server	Enter the IP address of the L2TP server.
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. In the redial period field, enter the number of seconds after which the device attempts to reconnect if it is disconnected.
Authentication Type	**Auto-negotiation**—The server sends a configuration request specifying the security algorithm set on it. The device then sends back authentication credentials with the security type sent by the server. **PAP**—Password Authentication Protocol (PAP) is used to connect to the ISP. **CHAP**—Challenge Handshake Authentication Protocol (CHAP) is used to connect to the ISP. **MS-CHAP or MS-CHAPv2**—Microsoft Challenge Handshake Authentication Protocol is used to connect to the ISP.

STEP 4 Click **Save**.

Configuring Optional Settings

To configure optional settings:

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

Host Name	Host name of the device.
Domain Name	Domain name for your network.
MTU	The maximum transmission 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, we recommend 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	MTU size.

STEP 2 Click **Save**.

Configuring a Mobile Network

Use the Mobile Network page to configure the device to connect to a Mobile Broadband USB modem that is connected to its USB interface.

To display the **Mobile Network** window, choose **Networking** > **WAN > Mobile Network**.

Global Settings

To install a USB modem:

STEP 1 Connect the USB modem. If the modem is supported, it is automatically detected and appears on the Mobile Network page.

STEP 2 Select **Auto** or **Manual** connection mode. Ethernet Connection Recovery works only if the Connect Mode is set to Auto.

- To enable your modem to establish a connection automatically, select **Auto** mode. If you select Auto, you must also either set a Connect on Demand time or select Keep Alive. Connect on Demand terminates the Internet connection after it is inactive for the specified period of time (Max Idle Time).

  If your Internet connection is terminated due to inactivity, the modem automatically establishes a connection when a user attempts to access the Internet. In the **Max Idle Time** field, enter the number of minutes of idle time that can elapse before the Internet connection terminates. Choosing **Keep Alive** keeps the connection up at all times.

- To connect or disconnect your modem connection manually, select **Manual** mode.

The device displays the current modem connection status that includes initializing, connecting, disconnecting, or disconnected.

STEP 3 Verify that the **Card Status** field shows that your mobile card is **Connected**.

These messages might also appear:

- Please set APN manually (because the device is unable to determine the access point name)
- Searching for service...
- no SIM card
- SIM locked
- SIM busy
- SIM ready
- pin code needed
- pin code error
- Card is locked

- Card is not activated
- Card initialized error
- error

Mobile Network Setup

If it is necessary to change any of the mobile network parameters in the **Mobile Network Setup** area, click the **Manual** radio button in the Configure Mode field. The device automatically detects supported modems and lists the appropriate configuration parameters. The SIM PIN can be modified in either Auto or Manual mode.

The Card Model shows the model of the modem in the USB port. Unsupported cards are reported as **unrecognized**.

To override any of the other parameters, select **Manual** and complete the following fields:

Field	Description
Access Point Name (APN)	Internet network that the mobile device is connecting to. Enter the access point name provided by your mobile network service provider. If you do not know the name of the access point, contact your service provider.
Dial Number	Dial number provided by your mobile network service provider for the Internet connection.
User Name Password	User name and password provided by your mobile network service provider.
SIM Check	SIM card check enable or disable.
SIM PIN	PIN code associated with your SIM card. This field is only displayed for GSM SIM cards.
Server Name	Name of the server for the Internet connection (if provided by your service provider).
Authentication	Authentication used by your service provider. The value can be changed by choosing the authentication type from the drop-down list. The default is Auto. If you do not know which type of authentication to use, select Auto.

Field	Description
Service Type	The most commonly available type of mobile data service connection based on your area service signal. If your location supports only one mobile data service, you can limit your preferred option, reducing connection setup times. The first selection always searches for HSPDA/3G/UMTS service and switches automatically to GPRS when it is available.
LTE Service	Long-term Evolution (LTE) Service setting. Select **Auto** for a signal based on the area service signal. Select **4G only** for only 4G signals. Select **3G only** for only 3G signals.

STEP 4 Click **Save** to save your settings

Bandwidth Cap Setting

The device monitors the data activity across the mobile network link and when it reaches a specific threshold, sends a notification.

To enable or disable Bandwidth Cap Tracking and set the limits:

STEP 1 Click **Enabled** or **Disabled**.

STEP 2 Select **Monthly Renewal Date** from the drop-down list to indicate which day of the month the bandwidth cap is reset.

STEP 3 In the **Monthly Bandwidth Cap** field, enter the maximum amount of data in megabytes that is allowed to pass before the device takes an action, such as sending an email to an administrator.

E-mail Setting

When the bandwidth data limit is reached, an email message can be sent to the administrator. To set up the target email address, check the **Email to** check box and click **Email Address**. For more information, see **Configuring E-mail Settings**.

When enabled by checking the box, email is sent when:

- Mobile network usage has exceeded a given percentage.

- The device fails over to the backup pathway and recovers.
- At every interval specified while a mobile network link is active.

Setting Failover and Recovery

While both an Ethernet and a mobile network link might be available, only one connection can be used to establish a WAN link at a time. When a WAN connection fails, the device attempts to bring up a connection on another interface. This feature is called Failover. When the primary WAN connection is restored, it drops the backup connection. This feature is called Recovery.

STEP 1 Choose **Networking > WAN > Failover & Recovery**.

STEP 2 Choose if your primary network connection is an ethernet WAN connection or a mobile network connection using a 3G USB dongle.

STEP 3 Click the **Failover to Secondary Enable** radio button to enable the device to failover from the primary network connection and restore connectivity using the secondary connection.

For example, your primary connection is an Ethernet WAN connection and the WAN link goes down. The device attempts to restore the connection using a 3G mobile network link on the USB interface. If **Failover to Secondary Enable** is not enabled, the secondary connection is disabled.

STEP 4 Click the **Recovery back to Primary Enable** radio button to enable the device to automatically revert to the primary connection and drop the secondary connection. The **WAN > Mobile Network** Connect Mode must be set to Auto to revert to a primary connection automatically.

STEP 5 In the **Failover Check Interval** field, enter the time (in seconds) after which the device must attempt to detect the presence of traffic on the secondary connection.

STEP 6 In the **Recovery Check Interval** field, enter the time (in seconds) after which the device must attempt to detect the presence of traffic on the primary connection. If the link is idle, the device pings a specified destination at the specified interval. If there is a reply to the ping packet, the device assumes that the link is up and attempts to revert to the primary network connection.

STEP 7 Click the **Switch back to Primary immediately when Primary is available** radio button or set a time in the **Switch back to Primary in a specific time range** field. If you choose a specific time range, set the start and end time.

STEP 8 In the **Recovery Ping** field, enter the number of times the device must ping the connection validation site after recovery. You can specify up to 5 recovery pings to the site. By default, the device will ping the validation site once.

STEP 9 In the **Connection Validation Site** field, choose the location to ping during failover and recovery validation. You can choose the device's gateway, DNS, or a custom IP address as the validation site. If you choose a custom site, enter the IPv4 or IPv6 address. By default, the device pings the default gateway to validate failover.

STEP 10 To troubleshoot your 3G mobile network connection, click the **3G Diagnostic Enable** radio button. Set the time when the device must test the 3G connection every day.

STEP 11 Click **Save**.

The WAN Interface table shows the status of the Ethernet WAN and mobile network link to the Internet. Click the **Status** hyper link to view the port detail.

WAN/USB Device Update

Use this page to load the USB module files that support USB dongles. Contact Cisco Support to acquire USB module files. The Dynamic Load USB Modem List shows the 3G and 4G USB dongle module files that are supported on the device.

To delete a module file, select the module from the Dynamic Load USB Modem List and click **Delete**.

To upload USB device firmware (a module) from the PC:

STEP 1 Verify that the USB dongle is not connected to the device.

STEP 2 Browse to and select the USB dongle module file.

STEP 3 Click **Import**.

STEP 4 Connect the USB dongle to the device.

Configuring the LAN Settings

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

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

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

Changing the Device Management IP Address

The local device management IP address of the device is static and defaults to 192.168.1.1.

To change the local device management IP address:

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

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

VLAN	The VLAN number.
Local IP Address	Local LAN IP address of the device. Ensure that this IP address is not in use by another device.
Subnet mask	Subnet mask for the local IP address. The default subnet mask is 255.255.255.0.

STEP 3 Click **Save**.

After changing the device IP address, your PC is no longer able to display Device Manager.

To display Device Manager, do one of the following:

- If DHCP is configured on the device, release and renew your PC IP address.
- Manually assign an IP address to your PC. The address must be on the same subnetwork as the device. For example, if you change the device 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.

Open a new browser window and enter the new IP address of the device to reconnect.

Configuring the DHCP Server

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

With DHCP enabled, the device assigns IP addresses to network devices on the LAN from a pool of IPv4 addresses. The device tests each address before it is assigned to avoid duplicate addresses on the LAN.

The default IP address pool is 192.168.1.100 to 192.168.1.149. To set a static IP address on a network device, use an IP address outside the pool. For example, assuming the DHCP pool is set to the default parameters, static IP addresses from 192.168.1.2 to 192.168.1.99 IP address pool can be used. This prevents conflicts with the DHCP IP address pool.

To configure DHCP settings:

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

STEP 2 (Optional) Select a VLAN to edit from the drop-down list.

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

Enable	Allows the device to act as the DHCP server in the network.
Disable	Disables DHCP on the device when you want to manually configure the IP addresses of all of your network devices.
DHCP Relay	Relays the IP addresses assigned by a another DHCP server to the network devices.

If you enabled the device DHCP server, enter this information:

Starting IP Address	The first address in the IP address pool. Any DHCP client joining the LAN is assigned an IP address in this range.
Maximum Number of DHCP Users	The maximum number of DHCP clients.
IP Address Range	(Read-only) The range of IP addresses available to the DHCP clients.
Client Lease time	Duration (in hours) that IP addresses are leased to clients.
Static DNS 1	IP address of the primary DNS server.
Static DNS 2	IP address of the secondary DNS server.
Static DNS 3	IP address of the tertiary DNS server.
WINS	IP address of the primary WINS server.

STEP 4 If you selected **DHCP Relay**, enter the address of the relay gateway in the **Remote DHCP Server** field. The relay gateway transmits DHCP messages to network device, including those on other subnetworks.

STEP 5 Click **Save**.

Configuring VLANs

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

The device has a default VLAN (VLAN 1) that cannot be deleted. You can create up to four other VLANs on the device.

To create a VLAN:

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

STEP 2 Click **Add Row**.

STEP 3 Enter this information:

VLAN ID	Numerical VLAN ID to assign to endpoints in the VLAN membership. The number you enter must be between 3 to 4094. VLAN ID 1 is reserved for the default VLAN, and is used for untagged frames received on the interface.
Description	A description that identifies the VLAN.
Inter VLAN Routing	Allows an end station in one VLAN to communicate with an end station in another VLAN.
Port 1 **Port 2** **Port 3** **Port 4**	You can associate VLANS on the device to the LAN ports on the device. By default, all LAN 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 interface 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**.

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

Configuring Static DHCP

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

To configure static DHCP:

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

STEP 2 From the **VLAN** drop-down menu, choose a VLAN number.

STEP 3 Click **Add Row**.

STEP 4 Enter this information:

Description	Description of the client.
IP Address	IP address of the device. The IP address assigned should be outside the pool of the DHCP addresses. Static DHCP assignment means the DHCP server assigns the same IP address to a defined MAC address every time the device is connected to the network. The DHCP server assigns the reserved IP address when the device using the corresponding MAC address requests an IP address.
MAC Address	MAC address of the device. The format for a MAC address is XX:XX:XX:XX:XX:XX where X is a number from 0 to 9 (inclusive) or a letter between A and F (inclusive).

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

Viewing DHCP Leased Clients

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

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

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

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

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

STEP 2 Click **Save**.

The DHCP server on the device always assigns the IP address shown when the device requests an IP address.

Configuring a DMZ Host

The device 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 device LAN IP address, but it cannot be identical to the IP address given to the LAN interface of this gateway.

To configure DMZ:

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

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

STEP 3 From the VLAN drop-down menu, choose the ID of the VLAN where DMZ is enabled.

STEP 4 In the **Host IP Address** field, enter the IP address of the DMZ host. The DMZ host is the endpoint that receives the redirected packets.

STEP 5 Click **Save**.

Configuring RSTP

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

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

STEP 2 Configure the following settings:

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

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

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

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

STEP 4 Click **Save**.

Port Management

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

To configure port speeds and flow control:

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

STEP 2 Configure this information:

Port	The port number.

Link	The port speed. If no device is connected to the port, this field displays **Down**.
Mode	Choose from the drop-down menu one of the following port speeds: • **Auto Negotiation**—The device and the connected device choose a common speed. • **10Mbps Half**—10 Mbps in both directions, but only one direction at a time. • **10Mbps Full**—10 Mbps in both directions simultaneously. • **100Mbps Half**—100 Mbps in both directions, but only one direction at a time. • **100Mbps Full**—100 Mbps in both directions simultaneously.
Flow Control	Check to enable flow control for this port. Flow control is the process of managing the rate of data transmission between two nodes to prevent a fast sender from outrunning a slow receiver. It provides a mechanism for the receiver to control the transmission speed, so that the receiving node is not overwhelmed with data from the transmitting node.

STEP 3 Click **Save**.

Cloning the MAC Address

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

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

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

To configure a MAC address clone:

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

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

STEP 3 To set the MAC address of the device WAN port, do one of the following:

- To set the MAC address of the WAN port to your PC MAC address, click **Clone My PC's MAC**.
- To specify a different MAC address, enter it in the **MAC Address** field.

STEP 4 Click **Save**.

Configuring Routing

Configure the routing options.

Configuring the Operating Mode

To configure the device operating mode:

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

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

Gateway	(Recommended) Click this button to set the device to act as a gateway. Keep this default setting if the device is hosting your network connection to the Internet and is performing the routing functions.

Router	(For advanced users only) Click this button to set the device to act as a router. Select this option if the device is on a network with other routers. Enabling the Router mode disables NAT (Network Address Translation) on the device.

STEP 3 Click **Save**.

Configuring Dynamic Routing

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

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

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

NOTE RIP is disabled by default on the device.

To configure dynamic routing:

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

STEP 2 Configure the following settings:

RIP	Check **Enable** to enable RIP. This allows the device 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. 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 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. The device supports up to 30 static routes.

Be careful not to introduce routing loops in your network.

To configure static routing:

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

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

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

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

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 & Wireless**—Click this button to direct packets to the LAN and wireless network. • **Internet (WAN)**—Click this button to direct packets to the Internet (WAN).

STEP 4 Click **Save**.

Viewing the Routing Table

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

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

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

Configuring Dynamic DNS

Dynamic DNS (DDNS) is an Internet service that allows routers with varying public IP addresses to be located using Internet domain names. To use DDNS, you must set up an account with a DDNS provider such as DynDNS.com, TZO.com, 3322.org, or noip.com.

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

To configure DDNS:

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

STEP 2 From the **DDNS Service** drop-down menu, choose **Disable** to disable this service or choose the DDNS service to use.

STEP 3 If you do not have a DDNS account, click the URL of the service to visit the selected DDNS service's website so that you can create an account.

STEP 4 Configure this information:

E-mail Address	(TZO.com and noip.com) Email address you used to create the DDNS account.
Username	(DynDNS.com and 3322.org) Username of the DDNS account.
Password	Password of the DDNS account.
Verify Password	(TZO.com, DynDNS.com, and noip.com) Password confirmation of the DDNS account.
Host Name	(DynDNS.com, 3322.org, and noip.com) Host name of the DDNS server.
Domain Name	(TZO.com) Name of the domain that is used to access the network.
Update Interval	Choose one of the following options to set the frequency with which to update the IP addess and the domain name to the DDNS server: **Never**—Never update. **Weekly**—Update every week at 00:MM on Monday, where MM is a randomly picked number between 0 and 59. By default, Weekly is chosen. **Semi-monthly**—Update on the first and the fifteenth day of the month at 00:MM, where MM is a randomly picked number between 0 and 59. **Monthly**—Update on the first day of the month at 00:MM, where MM is a randomly picked number between 0 and 59.
Internet IP Address	(Read-only) Internet IP address of the device.
Status	(Read-only) Indicates that the DDNS update has completed successfully or the account update information sent to the DDNS server failed.

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

STEP 6 Click **Save**.

Configuring the IP Mode

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

To select an IP mode:

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

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

LAN:IPv4, WAN:IPv4	Use IPv4 on the LAN and WAN ports.
LAN:IPv6, WAN:IPv4	Use IPv6 on the LAN ports and IPv4 on the WAN ports.
LAN:IPv6, WAN:IPv6	Use IPv6 on the LAN and WAN ports.
LAN:IPv4+IPv6, WAN:IPv4	Use IPv4 and IPv6 on the LAN ports and IPv4 on the WAN ports.
LAN:IPv4+IPV6, WAN:IPv4+IPv6	Use IPv4 and IPv6 on both the LAN and WAN ports.
LAN:IPv4, WAN:IPv6	Use IPv4 on the LAN and IPv6 on the WAN ports.

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

a. Click **Show Static 6to4 DNS Entry**.

b. In the **Domain** and **IP** fields, enter up to five domain-to-IP mappings.

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

STEP 4 Click **Save**.

Configuring IPv6

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

Configuring the IPV6 WAN Connection

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

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

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

See **Configuring the IP Mode** for instructions on how to set the IP mode.

Configuring DHCPv6

If your ISP provides you with a dynamically assigned address, configure the device as a DHCPv6 client.

To configure the device to be a DHCPv6 client:

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

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

STEP 3 Click **Save**.

Configuring a Static IPv6 WAN Address

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

To configure a static IPv6 WAN address:

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

STEP 2 From the **WAN Connection Type** menu, select **Static IPv6**.

STEP 3 Enter this information:

IPv6 Address	IPv6 address of the WAN port.
IPv6 Prefix Length	Length of the IPv6 prefix (typically defined by the ISP). The IPv6 network (subnet) is identified by the initial bits of the address called the prefix. All hosts in the subnetwork have the identical prefix. For example, in the IPv6 address `2001:0DB8:AC10:FE01::` the prefix is `2001`.
Default IPv6 Gateway	IPv6 address of the default gateway. This is typically the IP address of the server at the ISP.
Static DNS 1	IP address of the primary IPv6 DNS server.
Static DNS 2	IP address of the secondary IPv6 DNS server.

STEP 4 Click **Save**.

Configuring PPPoE IPv6 Settings

You can run IPv4 PPPoE, IPv6 PPPoE, or both. If you run both, your IPv6 WAN PPPoE settings must match your IPv4 WAN PPPoE settings. If they do not match, a message is displayed asking if you want to set the IPv6 protocol to match the IPv4 protocol. See **Configuring PPPoE**For more information.,

To configure the PPPoE IPv6 settings:

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

STEP 2 In the **WAN Connection Type** field, choose **PPPoE IPv6**.

STEP 3 Enter the following information (it might be necessary to contact your ISP to obtain your PPPoE login information):

Username	Username assigned to you by the ISP.
Password	Password assigned to you by the ISP.

Connect on Demand	If your ISP charges based on the amount of time that you are connected, select the radio button. When selected, the Internet connection is active only when traffic is present. If the connection is idle—that is, no traffic is flowing—the connection is closed. In the **Max Idle Time** field, enter the number of minutes that must elapse with no traffic detected on the link before the link is shut down.
Keep Alive	Keeps the WAN link up by sending a keep alive message through the port. In the redial period field, enter the number of seconds after which the device attempts to reconnect if it is disconnected.
Authentication Type	Authentication types: **Auto-negotiation**—A server sends a configuration request specifying the security algorithm set on the server. The device replies with its authentication credentials, including the security type sent by the server. **PAP**—Use the Password Authentication Protocol (PAP) to connect to the ISP. **CHAP**—Use Challenge Handshake Authentication Protocol (CHAP) to connect with the ISP. **MS-CHAP or MS-CHAPv2**—Use Microsoft Challenge Handshake Authentication Protocol to connect to the ISP.
Service Name	Name that your ISP might require to log onto the PPPoE server.
MTU	The maximum transmission unit (MTU) or the size of the largest packet that can be sent over the network. Unless a change is required by your ISP, we recommend that you choose **Auto**. The standard MTU value for Ethernet networks is 1500 bytes. For PPPoE connections, the value is 1492 bytes. If your ISP requires a custom MTU setting, choose **Manual.**

Size	MTU size. If your ISP requires a custom MTU setting, enter the MTU size.
Address Mode	Dynamic or static address mode. If you choose static, enter the IPv6 address in the next field.
IPv6 Prefix Length	IPv6 prefix length.
Default IPv6 Gateway	IP address of the default IPv6 gateway.
Static DNS 1	IP address of the primary DNS server.
Static DNS 2	IP address of the secondary DNS server.

STEP 4 Click **Save**.

Configuring IPv6 LAN Connections

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.

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

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

See **Configuring the IP Mode** for more information on how to set the IP mode.

To configure IPv6 LAN settings:

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

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

IPv6 Address	Enter the IPv6 address of the device. The default IPv6 address for the gateway is fec0::1 (or FEC0:0000:0000:0000:0000:0000:0000:0001). 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 addresses in this field.

STEP 3 Click **Save** or continue to configure IPv6 DHCP LAN settings.

STEP 4 Enter the following information to configure the DHCPv6 settings:

DHCP Status	Check to enable the DHCPv6 server. When enabled, the device assigns an IP address within a specified range and provides additional information to any LAN endpoint that requests DHCP addresses.
Domain Name	(Optional) Domain name of the DHCPv6 server.
Server Preference	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	IPv6 address of the primary DNS server on the ISP IPv6 network.
Static DNS 2	IPv6 address of the secondary DNS server on the ISP IPv6 network.
Client Lease Time	Client lease time duration (in seconds) for which IPv6 addresses are leased to endpoints on the LAN.

STEP 5 Choose **Networking** > **IPv6** > **IPv6 LAN Configuration**.

STEP 6 In the **IPv6 Address Pools Table**, click **Add Row**.

STEP 7 Enter this information:

Start Address	Starting IPv6 address of the pool.
End Address	Ending IPv6 address of the pool.
IPv6 Prefix Length	Prefix length that determines the number of common initial bits in the network addresses.

STEP 8 Click **Save**.

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

Configuring IPv6 Static Routing

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

Some ISPs require static routes to build a routing table instead of using dynamic routing protocols. Static routes do not require CPU resources to exchange routing information with a peer router.

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

To create a static route:

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

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

STEP 3 Enter this information:

Name	Route name.
Destination	IPv6 address of the destination host or network for this route.
Prefix Length	Number of prefix bits in the IPv6 address that define the destination subnet.
Gateway	IPv6 address of the gateway through which the destination host or network can be reached.
Interface	Interface for the route: **LAN**, **WAN**, or **6to4**.
Metric	Priority of the route. Choose 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 is listed in the routing table, but is not used by the device. Entering an inactive route is useful if the route is not available when you add the route. When the network becomes available, you can enable the route.

STEP 4 Click **Save**.

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

Configuring Routing (RIPng)

RIP Next Generation (RIPng) is a routing protocol based on the distance vector (D-V) algorithm. RIPng uses UDP packets to exchange routing information through port 521.

RIPng uses a hop count to measure the distance to a destination. The hop count is referred to as metric, or cost. The hop count from a router to a directly-connected network is 0. The hop count between two directly-connected routers is 1. When the hop count is greater than or equal to 16, the destination network or host is unreachable.

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

On the device, RIPng is disabled by default.

To configure RIPng:

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

STEP 2 Check **Enable**.

STEP 3 Click **Save**.

Configuring Tunneling

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

6 to 4 Tunneling

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

To configure 6-to-4 tunneling:

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

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

STEP 3 Choose the type of tunneling (**6to4** or **6RD** [Rapid Deployment]).

STEP 4 For 6RD Tunneling, choose **auto** or **manual**.

STEP 5 Enter the following information:

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

STEP 6 Click **Save**.

4 to 6 Tunneling

To configure 4-to-6 tunneling:

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

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

STEP 3 Enter the local WAN IPv6 address on the device.

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

STEP 5 Click **Save**.

Viewing IPv6 Tunnel Status

To view IPv6 tunnel status:

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

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

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

Configuring Router Advertisement

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

To configure the RADVD:

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

STEP 2 Enter this information:

RADVD Status	Check **Enable** to enable RADVD.
Advertise Mode	Select one of the following modes: **Unsolicited Multicast**—Send Router Advertisements (RAs) to all interfaces belonging to the multicast group. **Unicast only**—Restrict advertisements to well-known IPv6 addresses only (RAs are sent to the interface belonging to the known address only).
Advertise Interval	Advertise interval (4–1800) for the **Unsolicited Multicast**. 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	MTU size (0 or 1280 to 1500). The default is 1500 bytes. The Maximum Transmit Unit (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	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** > **Advertisement Prefixes**.

STEP 2 Click **Add Row**.

STEP 3 Enter this information:

IPv6 Prefix Type	Choose one of the following types: **6to4**—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	Prefix lifetime, or the length of time over which the requesting router is allowed to use the prefix.

STEP 4 Click **Save**.

7

Configuring the Wireless Network

This chapter describes how to configure the device wireless network.

Wireless Security

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

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

Wireless Security Tips

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

- Change the default wireless network name or SSID.

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

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

  When choosing names, do not use personal information (such as your Social Security number) because this information may be available for anyone to see when browsing for wireless networks.

- Change the default password.

  For wireless products such as access points, routers, and gateways, you are asked for a password when you want to change their settings. These devices have a default password. The default password is often **cisco**.

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

- Enable MAC address filtering.

  Cisco routers and gateways give you the ability to enable MAC address filtering. The MAC address is a unique series of numbers and letters assigned to every networking device.

  With MAC address filtering enabled, wireless network access is provided solely for wireless devices with specific MAC addresses. For example, you can specify the MAC address of each computer in your network so that only those computers can access your wireless network.

- Enable encryption.

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

  A network encrypted with WPA/WPA2 is more secure than a network encrypted with WEP, because WPA/WPA2 uses dynamic key encryption.

  To protect the information as it passes over the airwaves, enable the highest level of encryption supported by your network equipment.

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

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

General Network Security Guidelines

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

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

Cisco RV215W Wireless Networks

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

SSID Name	ciscosb1	ciscosb2	ciscosb3	ciscosb4
Enabled	Yes	No	No	No
SSID Broadcast	Enabled	Disabled	Disabled	Disabled
Security Mode	Disabled[1]	Disabled	Disabled	Disabled
MAC Filter	Disabled	Disabled	Disabled	Disabled

SSID Name	ciscosb1	ciscosb2	ciscosb3	ciscosb4
VLAN	1	1	1	1
Wireless Isolation with SSID	Disabled	Disabled	Disabled	Disabled
WMM	Enabled	Enabled	Enabled	Enabled
WPS Hardware Button	Enabled	Disabled	Disabled	Disabled

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

Configuring Basic Wireless Settings

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

To configure basic wireless settings:

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

STEP 2 In the **Radio** field, check **Enable** to turn on the wireless radio. By default there is only one wireless network enabled, **ciscosb1**.

STEP 3 In the **Wireless Network Mode** field, choose one of these options from the drop-down menu:

B/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 4 If you chose **B/G/N-Mixed**, **N-Only**, or **G/N Mixed**, in the **Wireless Band Selection** field, select the wireless bandwidth on your network (**20MHz** or **20/40MHz**). If you chose N-Only, you must use WPA2 security on your network. See **Configuring the Security Mode**.

STEP 5 In the **Wireless Channel** field, choose the wireless channel from the drop-down menu.

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

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

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

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

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

STEP 9 Click **Save**.

Editing the Wireless Network Settings

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

To configure wireless network settings:

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

STEP 2 Click the **Edit** button.

STEP 3 Configure these settings:

Enable SSID	Click **On** to enable the network.
SSID Name	Enter the name of the network.
SSID Broadcast	Check this box to enable SSID broadcast. If SSID broadcast is enabled, the wireless router advertises its availability to wireless-equipped devices in the range of the router.
VLAN	Choose the VLAN associated with the network.
Wireless Isolation with SSID	Check this box to enable wireless isolation within the SSID.
WMM (Wi-Fi Multimedia)	Check this box to enable WMM.
WPS Hardware Button	Check this box to map the device WPS button on the front panel to this network.

STEP 4 Click **Save**.

Configuring the Security Mode

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

Configuring WEP

The WEP security mode offers weak security with a basic encryption method that is not as secure as WPA. WEP may be required if your network devices do not support WPA.

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

To configure the WEP security mode:

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

STEP 2 Click **Edit Security Mode**.

The **Security Settings** page appears.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- **WPA-Personal**—WPA is part of the wireless security standard (802.11i) standardized by the Wi-Fi Alliance and was intended as an intermediate measure to take the place of WEP while the 802.11i standard was being prepared. WPA-Personal supports Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES) encryption.
- **WPA2-Personal**—(Recommended) WPA2 is the implementation of the security standard specified in the final 802.11i standard. WPA2 supports AES encryption and this option uses Preshared Key (PSK) for authentication.
- **WPA2-Personal Mixed**—Allows both WPA and WPA2 clients to connect simultaneously using PSK authentication.

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

To configure the WPA Personal security mode:

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

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

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

STEP 4 From the **Security Mode** menu, choose one of the three WPA Personal options.

STEP 5 (WPA-Personal only) In the **Encryption** field, choose one of the following options:

- **TKIP/AES**—Choose **TKIP/AES** to ensure compatibility with older wireless devices that may not support AES.
- **AES**—This option is more secure.

STEP 6 In the **Security Key** field, enter an alphanumeric phrase (8–63 ASCII characters or 64 hexadecimal digits). The password strength meter shows how secure the key is: below minimum, weak, strong, very strong, or secure. We recommend using a security key that registers on the strength meter as secure.

STEP 7 To show the security key as you are entering it, check the **Unmask Password** box.

STEP 8 In the **Key Renewal** field, enter the duration of time (600–7200 seconds) between key renewals. The default value is 3600.

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

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

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

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

- **WPA-Enterprise**—Allows you to use WPA with RADIUS server authentication.
- **WPA2-Enterprise**—Allows you to use WPA2 with RADIUS server authentication.
- **WPA2-Enterprise Mixed**—Allows both WPA and WPA2 clients to connect simultaneously using RADIUS authentication.

To configure the WPA Enterprise security mode:

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

STEP 2 Click **Edit Security Mode**.

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

STEP 4 From the **Security Mode** menu, choose one of the three WPA Enterprise options.

STEP 5 (WPA-Enterprise only) In the **Encryption** field, choose one of the following options:

- **TKIP/AES**—Choose **TKIP/AES** to ensure compatibility with older wireless devices that may not support AES.
- **AES**—This option is more secure.

STEP 6 In the **RADIUS Server** field, enter the IP address of the RADIUS server.

STEP 7 In the **RADIUS Port** field, enter the port used to access the RADIUS server.

STEP 8 In the **Shared Key** field, enter an alphanumeric phrase.

STEP 9 In the **Key Renewal** field, enter the duration of time (600–7200 seconds) between key renewals. The default value is 3600.

STEP 10 Click **Save** to save your settings.

STEP 11 Click **Back** to go back to the **Basic Settings** page.

Configuring MAC Filtering

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

To configure MAC filtering:

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

STEP 2 Click **Edit MAC Filtering**. The **Wireless MAC Filter** page appears.

STEP 3 In the **Edit MAC Filtering** field, check the **Enable** box to enable MAC Filtering for this SSID.

STEP 4 In the **Connection Control** field, choose the type of access to the wireless network:

- **Prevent**—Select this option to prevent devices with the MAC addresses listed in the **MAC Address Table** from accessing the wireless network. This option is selected by default.
- **Permit**—Select this option to allow devices with the MAC addresses listed in the **MAC Address Table** to access the wireless network.

STEP 5 To show computers and other devices on the wireless network, click **Show Client List**.

STEP 6 In the **Save to MAC Address Filter List** field, check the box to add the device to the list of devices to be added to the **MAC Address Table**.

STEP 7 Click **Add to MAC** to add the selected devices in the **Client List Table** to the **MAC Address Table**.

STEP 8 Click **Save** to save your settings.

STEP 9 Click **Back** to go back to the **Basic Settings** page.

Configuring Time of Day Access

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

To configure Time of Day Access:

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

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

STEP 3 In the **Active Time** field, check **Enable** to enable Time of Day Access.

STEP 4 In the **Start Time** and **Stop Time** fields, specify the time of day period when access to the network is allowed.

STEP 5 Click **Save**.

Configuring the Wireless Guest Network

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

- One guest network can be configured for each
- The guest network is configured as one of the four available SSIDs on the

- The guest network cannot be configured on the AP Management VLAN (VLAN ID 1).

To configure the guest network:

Create a New VLAN

STEP 1 In the Management Interface, choose **Networking** > **LAN** > **VLAN Membership**.

STEP 2 In the VLAN Setting Table, add a new VLAN for the guest network. For example, click **Add Row** and enter the following:

- **VLAN ID**—Enter a number for the VLAN (for example, **4**).
- **Description**—Enter a name for the VLAN (for example, **guest-net**).

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

Set Up the Guest Network

STEP 1 In the Management Interface, choose **Wireless** > **Basic Settings**.

STEP 2 In the Wireless Table, choose the SSID or network that you want to designate as the guest network.

STEP 3 Click **Edit**. Change the SSID name to reflect the guest designation (for example, *guest-net*).

STEP 4 Check the **SSID Broadcast** box so that the network will appear as an available wireless connection to clients searching for networks.

STEP 5 Check the **Guest Network** box to configure this SSID as the guest network.

STEP 6 Choose the VLAN you created for the guest network (or, if you have not yet created a network, select **Add New VLAN**).

STEP 7 Click **Save**. The system notifies you that the physical Ethernet ports on the are excluded from the VLAN that you have assigned to the guest network. In addition, Wireless Isolation with SSID and WMM are automatically enabled.

Configure the Password and Other Options

STEP 1 In the Management Interface, choose **Wireless** > **Basic Settings**.

STEP 2 Under the Wireless Table, click **Edit Guest Net**.

STEP 3 Enter a password that users will enter to access the guest network.

STEP 4 Enter the password again to confirm.

STEP 5 Enter the time, in minutes, that the guest connection will be available for users.

STEP 6 (Optional) To restrict bandwidth usage by the guest network, check **Enable Guest Bandwidth Restriction**. (QoS must be enabled first; click the link to the Bandwidth Management page if you need to configure QoS.) In the **Available Bandwidth** field, enter the percentage of bandwidth to allocate to the guest network.

STEP 7 Click **Save**.

Configuring Advanced Wireless Settings

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

To configure advanced wireless settings:

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

STEP 2 Configure these settings:

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

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 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 can transmit at all standard wireless rates (1 Mbps, 2 Mbps, 5.5 Mbps, 11 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, and 54 Mbps). In addition to B and G speeds, the supports N speeds. Other options are 1-2 Mbps, for use with older wireless technology, and All, when the can transmit at all wireless rates. The Basic Rate is not the actual rate of data transmission. If you want to specify the 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 automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the 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 automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the and a wireless client. The default is Auto.

CTS Protection Mode	The 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 in an environment with heavy 802.11b traffic. This function boosts the 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 to synchronize the wireless network. Enter a value between 40 and 3,500 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 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 and other remote WDS peers must be configured in the same wireless network mode, wireless channel, wireless band selection, and encryption types (None or WEP).

WDS is supported on one SSID only.

To configure a WDS:

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

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

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

To select repeaters from the Available Networks table, click **Show Site Survey** to display the **Available Networks Table**.

a. Click the check boxes to select up to three access points to use as repeaters.

b. Click **Connect** to add the MAC addresses of the selected access points to the MAC field.

You can also enter the MAC addresses of up to three access points to use as repeaters in the **MAC 1**, **MAC 2**, and **MAC 3** fields.

STEP 4 Click **Save**.

Configuring WPS

Configure WPS to allow WPS-enabled devices to easily and securely connect to the wireless network. Refer to your client device documentation for additional instructions on setting up WPS on your client device.

To configure WPS:

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

STEP 2 Select the wireless network on which to enable WPS from the **SSID** drop-down menu.

STEP 3 Check **WPS Enable** to enable WPS. To disable WPS, uncheck the box.

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

a. Click or press the WPS button on the client device and click the WPS icon on this page.

b. Enter the WPS PIN number of the client and click **Register**.

c. Enter a PIN number for the router; use the router PIN number indicated.

Device PIN Status—WPA device personal identification number (PIN) status.

Device PIN—Identifies the PIN of a device trying to connect.

PIN Lifetime—The lifetime of the key. If the time expires, a new key is negotiated.

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.

8

Configuring the Firewall

This chapter describes how to configure the firewall properties of the device.

Cisco RV215W Firewall Features

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

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

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

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

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

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

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

Configuring Basic Firewall Settings

To configure basic firewall settings:

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

STEP 2 Configure the following firewall settings:

Firewall	Check **Enable** to configure firewall settings.
DoS Protection	Check **Enable** to enable Denial of Service protection.
Block WAN Request	Blocks ping requests to the device from the WAN.
Web Access	Choose the type of web access that can be used to connect to the firewall: HTTP or HTTPS (secure HTTP).
Remote Management **Remote Access** **Remote Upgrade** **Allowed Remote IP Address** **Remote Management Port**	See **Configuring Remote Management**.
IPv4 Multicast Passthrough (IGMP Proxy)	Check **Enable** to enable multicast passthrough for IPv4.
IPv6 Multicast Passthrough (IGMP Proxy)	Check **Enable** to enable multicast passthrough for IPv6.
UPnP **Allow Users to Configure** **Allow Users to Disable Internet Access**	See **Configuring Universal Plug and Play**.
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** 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. 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. Click **Auto** to automatically block cookies, or click **Manual** and enter a specific port on which to block cookies.
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** 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** and enter a specific port on which to block proxy servers.

FTP ALG	Click **Auto** to use the default FTP port 21. Click **Manual** to enter the port number through which you want to direct FTP traffic on the device.

STEP 3 Click **Save**.

Configuring Remote Management

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

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

Remote Management	Check **Enable** to enable remote management.
Remote Access	Choose the type of web access that can be used to connect to the firewall: HTTP or HTTPS (secure HTTP).
Remote Upgrade	To allow remote upgrades of the device, check **Enable**.
Allowed Remote IP Address	Click the **Any IP Address** button to allow remote management from any IP address, or enter a specific IP address in the address field.
Remote Management Port	Enter the port on which remote access is allowed. The default port is 443. When remotely accessing the router, you must enter the remote management port as part of the IP address. For example: **https://<remote-ip>:<remote-port>**, or **https://168.10.1.11:443**

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

Configuring Universal Plug and Play

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

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

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

Managing Firewall Schedules

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

Adding or Editing a Firewall Schedule

Adding or Editing a Firewall Schedule

To create or edit a schedule:

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

STEP 2 Click **Add Row**.

STEP 3 In the **Name** field, enter a unique name to identify the schedule. This name is available on the Firewall Rule Configuration page in the **Select Schedule** list. (See **Configuring Access Rules**.)

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

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

STEP 6 Click **Save**.

Configuring Services Management

When you create a firewall rule, you can specify a service that is controlled by the rule. Common types of services are available for selection, and you can create your own custom services.

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

To create a custom service:

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

STEP 2 Click **Add Row**.

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

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

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

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

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

STEP 7 Click **Save**.

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

Configuring Access Rules

Configuring the Default Outbound Policy

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

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

To configure the default outbound policy:

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

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

Note: Ensure that IPv6 support is enabled on the device to configure an IPv6 firewall. See **Configuring IPv6**.

STEP 3 Click **Save**.

Reordering Access Rules

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

To reorder access rules:

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

STEP 2 Click **Reorder**.

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

STEP 4 Click **Save**.

Adding Access Rules

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

To create an access rule:

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

STEP 2 Click **Add Row**.

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

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

STEP 4 From the **Action** drop-down menu, choose the action:

- **Always Block**—Always block the selected type of traffic.
- **Always Allow**—Never block the selected type of traffic.
- **Block by schedule, otherwise allow**—Blocks the selected type of traffic according to a schedule.
- **Allow by schedule, otherwise block**—Allows the selected type of traffic according to a schedule.

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

- Domain Name System (DNS), UDP or TCP
- File Transfer Protocol (FTP)
- Hyptertext Transfer Protocol (HTTP)
- Secure Hypertext Transfer Protocol (HTTPS)
- Trivial File Transfer Protocol (TFTP)
- Internet Message Access Protocol (IMAP)
- Network News Transport Protocol (NNTP)
- Post Office Protocol (POP3)
- Simple Network Management Protocol (SNMP)
- Simple Mail Transfer Protocol (SMTP)
- Telnet
- STRMWORKS
- Terminal Access Controller Access-Control System (TACACS)
- Telnet (command)
- Telnet Secondary
- Telnet SSL
- Voice (SIP)

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

See **Configuring Services Management** for more information.

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

- **Any**—The rule applies to traffic originating on any host in the local network.
- **Single Address**—The rule applies to traffic originating on a single IP address in the local network. Enter the address in the **Start** field.

- **Address Range**—The rule applies to traffic originating from an IP address located in a range of addresses. Enter the starting IP address in the **Start** field, and the ending IP address in the **Finish** field.

STEP 8 In the **Log** field, specify whether the packets for this rule should be logged.

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

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

Choose **Never** to disable logging.

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

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

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

STEP 11 Click **Save**.

Creating an Internet Access Policy

The device supports several options for blocking Internet access. You can block all Internet traffic, block Internet traffic to certain PCs or endpoints, or block access to Internet sites by specifying keywords to block. If these keywords are found in the site's name (for example, web site URL or newsgroup name), the site is blocked.

Adding or Editing an Internet Access Policy

To create a Internet access policy:

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

STEP 2 Click **Add Row**.

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

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

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

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

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

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

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

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

b. From the **Type** drop-down menu, choose how to identify the PC (by MAC address, by IP address, or by providing a range of IP addresses).

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

- MAC address (xx:xx:xx:xx:xx:xx) of the PC to which the policy applies.
- The IP address of the of the PC to which the policy applies.
- The starting and ending IP addresses of the range of addresses to block (for example, 192.168.1.2-192.168.1.253).

STEP 8 To block traffic from specific websites:

a. In the **Website Blocking** table, click **Add Row**.

b. From the **Type** drop-down menu, choose how to block a website (by specifying the URL or by specifying a keyword that appears in the URL).

c. In the **Value** field, enter the URL or keyword used to block the website.

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

STEP 9 Click **Save**.

Configuring Port Forwarding

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

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

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

Some applications require that they receive data on a specific port or range of ports in order to function properly when external devices connect to them. The router must send all incoming data for that application only on the required port or range of ports.

The gateway has a list of common applications and games with corresponding outbound and inbound ports to open. You can also specify a port forwarding rule by defining the type of traffic (TCP or UDP) and the range of incoming and outgoing ports to open when enabled.

Configuring Single Port Forwarding

To add a single port forwarding rule:

STEP 1 Choose **Firewall** > **Single Port Forwarding**. A preexisting list of applications is displayed.

STEP 2 In the **Application** field, enter the name of the application for which to configure port forwarding.

STEP 3 In the **External Port** field, enter the port number that triggers this rule when a connection request from outgoing traffic is made.

STEP 4 In the **Internal Port** field, enter the port number used by the remote system to respond to the request it receives.

STEP 5 In the Interface drop-down menu, choose **Both (Ethernet & 3G)**, **Ethernet**, or **3G**.

STEP 6 From the **Protocol** drop-down menu, choose a protocol (**TCP**, **UDP**, or **TCP** & **UDP**).

STEP 7 In the **IP Address** field, enter the IP address of the host on the LAN side to which the specific IP traffic will be forwarded. For example, you can forward HTTP traffic to port 80 of the IP address of a web server on the LAN side.

STEP 8 In the **Enable** field, check the **Enable** box to enable the rule.

STEP 9 Click **Save**.

Configuring Port Range Forwarding

To add a port range forwarding rule:

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

STEP 2 In the **Application** field, enter the name of the application for which to configure port forwarding.

STEP 3 In the **External Port** field, specify the port number that will trigger this rule when a connection request from outgoing traffic is made.

STEP 4 In the **Start** field, specify the port number that begins the range of ports to forward.

STEP 5 In the **End** field, specify the port number that ends the range of ports to forward.

STEP 6 In the Interface drop-down menu, choose **Both (Ethernet & 3G)**, **Ethernet**, or **3G**.

STEP 7 From the **Protocol** drop-down menu, choose a protocol (**TCP**, **UDP**, or **TCP** & **UDP**).

STEP 8 In the **IP Address** field, enter the IP address of the host on the LAN side to which the specific IP traffic will be forwarded.

STEP 9 In the **Enable** field, check the **Enable** box to enable the rule.

STEP 10 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, which provides a level of security that port forwarding does not offer.

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

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

To add a port triggering rule:

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

STEP 2 In the **Application** field, enter the name of the application for which to configure port forwarding.

STEP 3 In the **Triggered Range** fields, enter the port number or range of port numbers that will trigger this rule when a connection request from outgoing traffic is made. If the outgoing connection uses only one port, enter the same port number in both fields.

STEP 4 In the **Forwarded Range** fields, enter the port number or range of port numbers used by the remote system to respond to the request it receives. If the incoming connection uses only one port, then specify the same port number in both fields.

STEP 5 In the Interface drop-down menu, choose **Both (Ethernet & 3G)**, **Ethernet**, or **3G**.

STEP 6 In the **Enable** field, check the **Enable** box to enable the rule.

STEP 7 Click **Save**.

9

Configuring VPN

This chapter describes how to configure VPN and security for the device.

VPN Tunnel Types

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

Remote access using PPTP

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

Remote Access with Cisco QuickVPN

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

Site-to-Site VPN

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

VPN Clients

VPN client software is required to establish a VPN tunnel between the router and remote endpoint. Your device supports Cisco QuickVPN and PPTP VPN clients.

Configuring PPTP

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

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

To configure the PPTP VPN service:

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

STEP 2 Enter the following information:

PPTP Server	Check to enable the PPTP server.
IP Address for PPTP Server	Enter the IP address of the PPTP server.
IP Address for PPTP Clients	Enter the IP address range of PPTP clients.
MPPE Encryption	Check the **Enable** box to enable MPPE encryption. Microsoft Point-to-Point Encryption (MPPE) is used when users set up and use a PPTP VPN client to connect to the device.

STEP 3 Click **Save**.

Configuring QuickVPN

STEP 1 Add the QuickVPN users on the **VPN > VPN Clients** page. See **Importing VPN Client Settings** and **Creating and Managing QuickVPN Users**.

STEP 2 Instruct users to obtain the free Cisco QuickVPN software from Cisco.com, and install it on their computers. See **Using the Cisco QuickVPN Software**

STEP 3 To enable access using Cisco QuickVPN on your device, you must enable remote management to open port 443 for SSL. See **Configuring Basic Firewall Settings**.

Configuring NetBIOS over VPN

To enable NetBIOS over VPN:

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

STEP 2 Click **Save**.

Creating and Managing PPTP Users

To create PPTP users:

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

STEP 2 Enter this information:

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

STEP 3 Click **Save**.

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

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

Creating and Managing QuickVPN Users

To create QuickVPN users:

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

STEP 2 Enter this information:

STEP 3 Click **Save**.

To edit settings for a QuickVPN user, check the box and click **Edit**. Make changes and click **Save**.

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

Importing VPN Client Settings

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

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

For example, the following specifies the settings of two users to import:

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

CAUTION Importing VPN client settings deletes existing settings.

To import VPN client settings:

STEP 1 Click **Browse** to locate the file.

STEP 2 Click **Import** to load the file.

STEP 3 When prompted, to delete existing VPN user settings and import the settings in the CSV file, click **Yes**.

Configuring Basic Site-to-Site IPsec VPN Settings

The device supports site-to-site VPN for a single gateway-to-gateway VPN tunnel. In this configuration, the device creates a secure connection to another VPN-enabled router. For example, you can configure the device at a branch site to connect to the router at the corporate site, so that the branch site can securely access the corporate network.

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

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

STEP 2 In the **Connection Name** field, enter a name for the VPN tunnel.

STEP 3 In the **Pre-Shared Key** field, enter the pre-shared key, or password, that will be exchanged between the two routers. It must be between 8 and 49 characters.

STEP 4 In the **Endpoint Information** fields, enter the following information:

- **Remote Endpoint**—Choose the way the remote endpoint, or the router to which the device will connect, is identified. For example, by an IP address such as 192.168.1.1, or by a fully qualified domain name such as cisco.com.
- **Remote WAN (Internet) IP Address**—Enter the public IP address or domain name of the remote endpoint.
- **Redundancy Endpoint**—To enable the device to switch to an alternate gateway when the primary VPN connection fails, check the **Enable** check box. Enter the WAN IP address or the FQDN for the redundancy endpoint.
- **Local WAN (Internet) IP Address**—Enter the public IP address or domain name of the local endpoint (device).

STEP 5 In the **Secure Connection Remote Accessibility** fields, enter the following information:

- **Remote LAN (Local Network) IP Address**—Enter the private network (LAN) address of the remote endpoint. This is the IP address of the internal network at the remote site.
- **Remote LAN Subnet Mask**—Enter the private network (LAN) subnet mask of the remote endpoint.
- **Local LAN (Local Network) IP Address**—Enter the private network (LAN) address of the local network. This is the IP address of the internal network on the device.
- **Local LAN (Local Network) Subnet Mask**—Enter the private network (LAN) subnet mask of the local network (device).

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

STEP 6 Click **Save**.

Viewing Default Values

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

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

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

For more information on these values, see **Configuring Advanced VPN Parameters**.

Configuring Advanced VPN Parameters

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

Managing IKE Policies

The Internet Key Exchange (IKE) protocol dynamically exchanges keys between two IPsec hosts. You can create IKE policies to define the security parameters such as authentication of the peer and encryption algorithms to be used in this process. Be sure to use compatible encryption, authentication, and key-group parameters for the VPN policy.

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

STEP 2 In **VPN Policy Table**, checking the box in the VPN connection row allows you to perform the following tasks:

- **Add Row** or **Edit**—Edit properties of the IKE policy. See **Adding or Editing IKE Policies**.
- **Enable**—Enable the policy.
- **Disable**—Disable the policy.
- **Delete**—Delete the policy.

NOTE You cannot delete an IKE policy if it is being used in a VPN policy. You must first disable and delete the VPN policy in the **VPN Policy Table**.

- **Add Row**—Add an IKE policy. See **Adding or Editing IKE Policies**.

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

STEP 3 Click **Save**.

Adding or Editing IKE Policies

STEP 1 When adding or editing IKE policies, configure the following settings:

- **Policy Name—**Enter a unique name for the policy for identification and management purposes.
- **Exchange Mode—**Choose one of the following options:
  - **Main**—Negotiates the tunnel with higher security, but is slower.
  - **Aggressive**—Establishes a faster connection, but with lowered security.
- **Local Identifier**—Local IKE identifier.
- **Remote Identifier**—Remote IKE identifier.
- **Redundancy Identifier**—The unique identifier for the alternate backup endpoint used to restore the connection if the original VPN connection fails.

STEP 2 In the **IKE SA Parameters** section, the Security Association (SA) parameters define the strength and mode for negotiating the SA. You can configure the following settings:

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

- **MD5**
- **SHA-1**
- **SHA2-256**

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

- **Pre-Shared Key—**Enter the key in the space provided. Note that the double-quote character (“) is not supported in the pre-shared key.
- **Diffie-Hellman (DH) Group—**Specify the DH Group algorithm, which is used when exchanging keys. The DH Group sets the strength of the algorithm in bits. Ensure that the DH Group is configured identically on both sides of the IKE policy.
- **SA Lifetime—**Enter the interval, in seconds, after which the Security Association becomes invalid.
- **Dead Peer Detection—**Check the **Enable** box to enable this feature, or uncheck the box to disable it. Dead Peer Detection (DPD) is used to detect whether the peer is alive or not. If the peer is detected as dead, the router deletes the IPsec and IKE Security Association. If you enable this feature, also enter these settings:
  - **DPD Delay—**Enter the interval, in seconds, between consecutive DPD R-U-THERE messages. DPD R-U-THERE messages are sent only when the IPsec traffic is idle.
  - **DPD Timeout—**Enter the maximum time that the device should wait to receive a response to the DPD message before considering the peer to be dead.

STEP 3 Check the **XAUTH Type Enable** check box to configure extended authentication for your IPsec VPN policy. Provide the authentication username and password.

STEP 4 Click **Save**.

Managing VPN Policies

To manage VPN policies:

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

STEP 2 In the **VPN Policy Table**, checking the box in the VPN connection row allows you to perform the following tasks:

- **Add Row** or **Edit**—Edit properties of the VPN policy. See **Adding or Editing VPN Policies**.
- **Enable**—Enable the policy.
- **Disable**—Disable the policy.
- **Delete**—Delete the policy.
- **Add Row**—Add a VPN policy. See **Adding or Editing VPN Policies**.

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

STEP 3 Click **Save**.

Adding or Editing VPN Policies

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

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

- **Policy Name—**Enter a unique name to identify the policy.
- **Policy Type—**Choose one of the following options:
  - **Auto Policy**—Some parameters for the VPN tunnel are generated automatically. This requires using the IKE (Internet Key Exchange) protocol to perform negotiations between the two VPN endpoints.
  - **Manual Policy**—All settings (including the keys) for the VPN tunnel are manually input for each end point. No third-party server or organization is involved.
- **Remote Endpoint—**Select the type of identifier that you want to provide for the gateway at the remote endpoint: **IP Address** or **FQDN** (Fully Qualified Domain Name). Enter the identifier in the space provided.
- **Redundancy Endpoint—** To enable the device to switch to an alternate gateway when the primary VPN connection fails, check the **Enable** check box. Enter the WAN IP address or the FQDN for the redundancy endpoint.

To automatically revert to the primary VPN when the connnection is restored, check the **Rollback enable** check box.

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

- **Local/Remote IP**—Select the type of identifier that you want to provide for the endpoint:
  - **Single**—Limits the policy to one host. Enter the IP address of the host that will be part of the VPN in Start IP Address field. Enter the IP address in the **Start Address** field.
  - **Subnet**—Allows an entire subnet to connect to the VPN. Enter the network address in the Start IP Address field, and enter the Subnet Mask in the Subnet Mask field. Enter the subnet's network IP address in the **Start Address** field. Enter the subnet mask, such as 255.255.255.0, in the **Subnet Mask** field. The field automatically displays a default subnet address based on the IP address.

    IMPORTANT: Make sure that you avoid using overlapping subnets for remote or local traffic selectors. Using these subnets would require adding static routes on the router and the hosts to be used. For example, a combination to avoid would be:

    Local Traffic Selector: 192.168.1.0/24

    Remote Traffic Selector: 192.168.0.0/16

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

- **SPI-Incoming, SPI-Outgoing**—Enter a hexadecimal value between 3 and 8 characters; for example, 0x1234.
- **Encryption Algorithm**—Select the algorithm used to encrypt the data:
  - DES
  - 3DES
  - AES-128
  - AES-192
  - AES-256
- **Key-In**—Enter the encryption key of the inbound policy. The length of the key depends on the encryption algorithm chosen:
  - DES—8 characters

  - 3DES—24 characters
  - AES-128—16 characters
  - AES-192—24 characters
  - AES-256—32 characters
- **Key-Out**—Enter the encryption key of the outbound policy. The length of the key depends on the encryption algorithm chosen, as shown above.
- **Integrity Algorithm**—Select the algorithm used to verify the integrity of the data:
  - MD5
  - SHA-1
  - SHA2-256
- **Key-In**—Enter the integrity key (for ESP with Integrity-mode) for the inbound policy. The length of the key depends on the algorithm chosen:
  - MD5—16 characters
  - SHA-1—20 characters
  - SHA2-256—32 characters
- **Key-Out**—Enter the integrity key (for ESP with Integrity-mode) for the outbound policy. The length of the key depends on the algorithm chosen, as shown above.

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

- **SA-Lifetime**—Enter the duration of the Security Association in seconds. After the specified number of seconds passes, the Security Association is renegotiated. The default value is 3600 seconds. The minimum value is 300 seconds.
- **Encryption Algorithm—**Select the algorithm used to encrypt the data.
- **Integrity Algorithm—**Select the algorithm used to verify the integrity of the data.
- **PFS Key Group—**Check the **Enable** box to enable Perfect Forward Secrecy (PFS) to improve security. While slower, this protocol helps to prevent eavesdroppers by ensuring that a Diffie-Hellman exchange is performed for every phase-2 negotiation.

- **Select IKE Policy—**Choose the IKE policy that will define the characteristics of phase 1 of the negotiation. Click **View** to view or edit the existing IKE policy that is configured on the device.

Configuring Certificate Management

The device 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 device.

Generating a New Certificate

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

To generate a certificate:

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

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

STEP 3 Click **Generate Certificate**.

Importing Certificates

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

To import a certificate:

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

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

STEP 3 Click **Browse** and locate the certificate file.

STEP 4 Click **Install Certificate**.

Exporting Certificates for Admin

You can export the certificate for administrator to a folder on your computer or to an external location on a USB drive.The certificate for administrator contains the private key and should be stored in a safe place as a backup. If the device configuration is reset to the factory default settings, this certificate can be imported and restored on the router.

To export a certificate for Admin:

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

STEP 2 To export the certificate to your computer, click **Export for Admin**. Device Manager saves the admin.pem file in the C:\Documents and Settings\userid\My Documents\Downloads.

To export the certificate to an external USB drive, click **Export to USB for Admin**.

Exporting Certificates for Client

You can export certificates for clients to your computer or to an external location on a USB drive. The certificate for the client allows QuickVPN users to securely connect to the Cisco RV215W. QuickVPN users must place the certificate in the install directory of the QuickVPN client.

To export a certificate for client:

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

STEP 2 To export the certificate to your computer, click **Export for Client**. On a PC, Device Manager saves the client.pem file in the C:\Documents and Settings\userid\My Documents\Downloads.

To export the certificate to an external USB drive, click **Export to USB for Client**.

Configuring VPN Passthrough

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

To configure VPN passthrough:

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

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

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

STEP 3 Click **Save**.

10

Configuring Quality of Service (QoS)

The Cisco RV215W lets you configure the following quality of service (QoS) features:

Quality of service (QoS) assigns priority to various applications, users, or data flows, or guarantees a level of performance to a data flow. This guarantee is important when the network capacity is insufficient. Especially for real-time streaming multimedia applications such as voice-over-IP, online games, and IP-TV, which often require fixed bit rates and are delay sensitive, and in networks where the capacity is a limited resource, for example in cellular data communication.

Configuring Bandwidth Management

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

Configuring Bandwidth

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

To set the upstream and downstream bandwidth:

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

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

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

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

STEP 4 Click **Save**.

Configuring Bandwidth Priority

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

To configure bandwidth priority:

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

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

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

STEP 4 Enter this information:

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

STEP 5 Click **Save**.

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

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

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

Configuring QoS Port-Based Settings

You can configure QoS settings for every LAN port on the Cisco RV215W. The device supports 4 priority queues that allow for traffic prioritization per physical switch port.

To configure QoS settings for the device LAN ports:

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

STEP 2 For each port in the **Ethernet QoS Port-Based Settings** table, enter this 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).
Default Traffic Forwarding Queue for Untrusted Devices	Choose a priority level for outbound traffic (1 to 4).

STEP 3 For each port in the **3G QoS Port-Based Settings** table, enter this 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).
Default Traffic Forwarding Queue for Untrusted Devices	Choose a priority level for outbound traffic (1 to 4).

STEP 4 Click **Save**.

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

Configuring CoS Settings

Use the link to the QoS Port-Based Settings Page to map the CoS priority setting to the QoS queue.

To map CoS priority settings to the traffic forwarding queue:

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

STEP 2 Choose the **Ethernet** or **3G** radio button.

STEP 3 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 4 Click **Save**.

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

Configuring DSCP Settings

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

To configure DSCP-to-QoS queue mapping:

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

STEP 2 Choose the **Ethernet** or **3G** radio button.

STEP 3 Choose whether to only list RFC values or to list all DSCP values in the **DSCP Settings Table** by clicking the relevant button.

STEP 4 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 5 Click **Save**.

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

11

Administering Your Router

This chapter describes the administration features of the device, including user creation, network management, system diagnostics and logs, date and time, and other settings.

Setting Password Complexity

Your device can enforce minimum password complexity requirement for password changes.

To configure password complexity settings:

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

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

STEP 3 Configure password complexity settings:

Minimum Password Length	Enter the minimum password length (0 to 64 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 contains 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 (1–365). The default is 180 days.

STEP 4 Click **Save**.

Configuring User Accounts

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

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

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

To configure the user accounts:

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

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

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

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

STEP 4 To import user names and passwords from a CSV file:

a. In the **Import User Name & Password** field, click **Browse**.

b. Locate the file and click **Open**.

c. Click **Import**.

STEP 5 Enter the old password.

STEP 6 Click **Save**.

Setting the Session Timeout Value

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

To configure session timeout:

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

STEP 2 In the **Administrator Inactivity Timeout** field, enter the number, in minutes, before a session times out due to inactivity. Choose **never** to allow the administrator to stay logged in permanently.

STEP 3 In the **Guest Inactivity Timeout** field, enter the number, in minutes, before a session times out due to inactivity. Choose **never** to allow the administrator to stay logged in permanently.

STEP 4 Click **Save**.

Configuring Simple Network Management (SNMP)

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

Configuring SNMP System Information

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

Before you can use SNMP, install SNMP software on your computer. The device supports only SNMPv3 for SNMP management and SNNPv1/2/3 for SNMP trap messages.

To enable SNMP:

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

STEP 2 Check **Enable** to enable SNMP.

STEP 3 Enter this information:

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

STEP 4 Click **Save**.

Editing SNMPv3 Users

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

To configure SNMPv3 settings:

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

STEP 2 Under **SNMPv3 User Configuration**, configure the following settings:

UserName	Select the account to configure (**admin** or **guest**).
Access Privilege	Displays the access privileges of the selected user account.
Security Level	Choose the SNMPv3 security level: **No Authentication and No Privilege**—Does not require any Authentication and Privacy. **Authentication and No Privilege**—Submit only Authentication algorithm and password. **Authentication and Privilege**—Submit Authentication/privacy algorithm and password.
Authentication Algorithm Server	Select the type of authentication algorithm (**MD5** or **SHA**).

Authentication Password	Enter the authentication password.
Privacy Algorithm	Choose the type of privacy algorithm (**DES** or **AES**).
Privacy Password	Enter the privacy password.

STEP 3 Click **Save**.

Configuring the SNMP Traps

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

To configure the traps:

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

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

IP Address	Enter the IP address of the SNMP manager or trap agent.
Port	Enter the SNMP trap port of the IP address to which the trap messages will be sent.
Community	Enter the community string to which the agent belongs. Most agents are configured to listen for traps in the Public community.
SNMP Version	Select the SNMP version: **v1**, **v2c**, or **v3**.

STEP 3 Click **Save**.

Configuring TR069 Settings

TR-069 is a DSL Forum specification for CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices. As a bidirectional SOAP/HTTP-based protocol, it provides the communication between customer-premises equipment (CPE) and Auto Configuration Servers (ACS).

To configure general TR-069 settings:

STEP 1 Click **Administration** > **TR069**, the TR069 page opens.

STEP 2 In the **Status** area, click **Enable** to enable the TR069 server, and click **Disable** to disable it.

STEP 3 Specify the settings of the ACS remote management servers

ACS URL	Enter the URL of the ACS remote management server.
ACS Username	Enter the username to log in to the ACS remote management server.
ACS Password	Enter the password to log in to the ACS remote management server

STEP 4 Specify the CPE settings for TR069 remote management:

Connection Request Port	Enter the port number used to request the connection to TR-069.
Connection Request Username	Enter the username of the remote management server in order to send the connection requests to CPE.
Connection Request Password	Enter the password of the remote management server in order to send the connection requests to CPE.

STEP 5 In the **Periodic Inform Enable** area, click **Enable** to enable sending the inform packets, and click **Disable** to disable it.

STEP 6 In the **Periodic Inform Interval** area, enter the interval value of sending the inform packets ranging from 0 to 86400. The default is 86400 seconds.

STEP 7 In the **Provisioning Code** area, enter the provision code used by the ACS to provision the CPE.

Using Diagnostic Tools

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

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

Network Tools

Use network tools to troubleshoot the network.

Using PING

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

To use PING:

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

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

STEP 3 Click **Ping**. The ping results appear. These results tell you whether the device is reachable.

STEP 4 Click **Close** when done.

Using Traceroute

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

To use Traceroute:

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

STEP 2 In the **IP Address / Domain Name** field, enter the IP address to trace.

STEP 3 Click **Traceroute**. The Traceroute results appear.

STEP 4 Click **Close** when done.

Performing a DNS Lookup

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

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

To use the Lookup tool:

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

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

STEP 3 Click **Lookup**. The nslookup results appear.

STEP 4 Click **Close** when done.

Configuring Port Mirroring

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

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

To configure port mirroring:

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

STEP 2 In the **Mirror Source** field, select the ports to mirror.

STEP 3 From the **Mirror Port** drop-down menu, choose a mirror port. If you use a port for mirroring, do not use it for any other traffic.

STEP 4 Click **Save**.

Configuring Logging

The Cisco RV215W allows you to configure logging options.

Configuring Logging Settings

To configure logging:

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

STEP 2 In the **Log Mode** field, check **Enable**.

STEP 3 Click **Add Row**.

STEP 4 Configure the following settings:

Remote Log Server	Enter the IP address of the log server that will collect logs.
Log Severity for Local Log and Email	Click to choose the severity of logs you want to configure. Note that all log types above a selected log type are automatically included and you cannot deselect them. For example, choosing error logs automatically includes emergency, alert, and critical logs in addition to error logs. 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. Choosing this severity uses large amounts of logs to be generated and is not recommended during normal router operation.
Enable	To enable these logging settings, check this box.

STEP 5 Click **Save**.

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

Configuring E-mail Settings

You can configure the Cisco RV215W to send event logs, new firmware alerts and 3G alerts by e-mail. We recommend that you set up a separate e-mail account for sending and receiving e-mail alerts.

To configure e-mail settings:

STEP 1 Choose **Administration** > **Logging** > **E-mail Settings**.

STEP 2 In the **E-mail Alert Configuration** section:

- To enable sending 3G alerts by e-mail, check the **3G E-mail Alert Enable** check box.
- To enable sending logs by e-mail, check the **E-mail Logs Enable** check box**.** Ensure that you have set severity for the events that you want to log. For more information, see **Configuring Logging Settings**. The **Minimum E-mail Log Severity** field displays the severity of logs that you want to capture. To change log severity, click **Configure Severity**.

  In the **Send E-mail Logs by Schedule** section, choose if you want to send e-mail **Hourly**, **Daily**, or **Weekly**. If you choose **Never**, logs are not sent. If you chose a weekly schedule, choose the day of the week to e-mail the logs. If you chose a daily or weekly schedule, choose the time of day when the device must e-mail the logs.

STEP 3 In the **E-mail Settings** section, enter the following information to configure settings for your e-mail alerts:

E-mail Server Address	Enter the address of the SMTP server. This is the mail server associated with the e-mail account that you have setup (for example, mail.companyname.com).
E-mail Server Port	Enter the SMTP server port. If your e-mail provider requires a special port for email, enter it here. Otherwise, use the default (25).
Return E-mail Address	Enter the return e-mail address that the Cisco RV215W will send messages to if alerts sent from the router are not delivered to the Send-to e-mail address.

Send to E-mail Address (1)	Enter the e-mail address to which to send alerts (for example, logging@companyname.com).
Send to E-mail Address (2) (Optional)	Enter an additional e-mail address to which to send alerts.
Send to E-mail Address (3) (Optional)	Enter an additional e-mail address to which to send alerts.
E-mail Encryption (SSL)	To enable email encryption, check **Enable**.
Authentication with SMTP Server	If the SMTP (mail) server requires authentication before accepting connections, choose the type of authentication from the drop-down menu: **None**, **LOGIN**, **PLAIN**, and **CRAM-MD5**.
E-mail Authentication Username	Enter the e-mail authentication username (example, logging@companyname.com).
E-mail Authentication Password	Enter the e-mail authentication password (for example, the password used to access the e-mail account you have set up to receive alerts).
E-mail Authentication Test	Click **Test** to test e-mail authentication.

STEP 4 In the **Send E-Mail Logs by Schedule** section, configure the following settings:

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

STEP 5 Click **Save**.

Configuring Bonjour

Bonjour is a service advertisement and discovery protocol. On the Cisco RV215W, Bonjour only advertises the default services configured on the device when Bonjour is enabled.

To enable Bonjour:

STEP 1 Choose **Administration** > **Bonjour**.

STEP 2 Check **Enable** to enable Bonjour.

STEP 3 To enable Bonjour for a VLAN listed in the **Bonjour Interface Control Table**, check the corresponding **Enable Bonjour** box.

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

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

STEP 4 Click **Save**.

Configuring Date and Time Settings

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

To configure NTP and time settings:

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

STEP 2 Configure this information:

Time Zone	Select your time zone, relative to Greenwich Mean Time (GMT).

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

STEP 3 Click **Save**.

Backing Up and Restoring the System

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

When the firewall is working as configured, you can back up the configuration for restoring later. During backup, your settings are saved as a file on your PC. You can restore the firewall settings from this file.

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

Backing Up the Configuration Settings

To back up or restore the configuration:

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

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

Startup configuration	Select this option to download the startup configuration. The startup configuration is the most current running configuration that the device uses. If the router startup configuration has been lost, use this page to copy the backup configuration to the startup configuration and keep all their previous configuration information intact. You can download the startup configuration to other Cisco RV215W devices for easy deployment.
Mirror configuration	Select this option to instruct the device to back up the startup configuration after 24 hours of operation without any change in the startup configuration.
Backup configuration	Select this option to back up the current configuration settings.

STEP 3 To download the backup file to your computer, click **Download**.

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

To save a backup file to a location on a USB drive, click **Save to USB.**

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

Restoring the Configuration Settings

You can restore a previously saved configuration file:

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

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

STEP 3 You can upload the configuration file from your PC or from an external USB device.

To upload from your computer, click the **PC** radio button. Click **Browse** to locate the file. Select the file and click **Open**.

To upload from a location on a USB drive, click the **USB** radio button. Click **Show USB** to display all connected USB devices. Locate the file on the USB drive and click **Open**.

NOTE Your device supports NTFS in read-only mode and supports the FAT and FAT32 file formats in read/write mode on USB devices.

STEP 4 Click **Start to Upload**.

The device uploads the configuration file and uses the settings it contains to update the startup configuration. The device then restarts and uses the new configuration.

Copying the Configuration Settings

Copy the startup configuration to the backup configuration to ensure that you have a backup copy in case you forget your username and password and are locked out of Device Manager. In this case, the only way to get back into Device Manager is to reset the device to factory default.

The backup configuration file remains in memory and allows the backed-up configuration information to be copied to the startup configuration, which restores all of the settings.

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

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

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

STEP 3 Click **Start to Copy**.

Generating an Encryption Key

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

To generate an encryption key:

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

STEP 2 Click **Show Advanced Settings**.

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

STEP 4 Click **Save**.

Upgrading Firmware or Changing the Language

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

CAUTION During a firmware upgrade, do not try to go online, turn off the device, shut down the PC, or interrupt the process in any way until the operation is complete. This process takes about a minute, including the reboot process. Interrupting the upgrade process at specific points when the flash memory is being written to may corrupt it and render the router unusable.

Upgrading Firmware Automatically

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

STEP 2 In the **Automatic Firmware Upgrade** section, select how frequently you want the device to check for updates to the firmware, in the **Interval - Check every** field.

STEP 3 In the **Automatically Upgrade** field, choose if you want to upgrade to the latest firmware immediately after a new version is detected, or at a specified time.

STEP 4 To be notified when new firmware is available or after the latest firmware is upgraded, check one of the following check boxes:

- **Notify via Admin GUI—** Receive notifications on the RV215W Administration GUI when you log on the next time.
- **Email to** — Receive notifications through e-mail alerts. Click **Email Address** to configure e-mail settings. This check box is dimmed if **New Firmware E-mail Alert** is not enabled. For more information, see **Configuring E-mail Settings**.

STEP 5 Click **Save**.

Upgrading Firmware/Configuration Automatically from a USB Device

To upgrade your firmware and configuration from a USB device automatically:

STEP 1 Choose **Enable** in the **Upgrade from USB drive when device powers on** field.

With this zero-touch deployment setting, if the USB device is inserted:

- The firmware on your device is upgraded automatically when the device is powered on.
- The configuration file is uploaded automatically when the device is powered on and when the device is reset to factory default settings.

STEP 2 Click **Save**.

Upgrading Firmware Manually

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

STEP 2 In the **Manual Firmware/Language Upgrade** section, click the **Firmware Image** radio button in the **File Type** field.

STEP 3 Download the latest firmware to your PC or to a USB device. To download the latest version of the firmware from cisco.com to a USB device, click **Start Download** in **Save to USB from cisco.com**.

STEP 4 To upgrade to the latest firmware version, choose one of the following options to upgrade from:

- **cisco.com**—Download the firmware from the cisco.com website.
- **PC**—Click **Browse** to locate and select the downloaded firmware on your computer.
- **USB**—Click **Show USB** to display all the files on your USB device, in the **USB Content Table**. Locate and select the firmware file.

NOTE Your device supports NTFS in read-only mode and supports the FAT and FAT32 file formats in read/write mode on USB devices.

CAUTION Resetting the device to default factory settings erases all of your configuration settings.

STEP 5 Click **Start Upgrade**.

After the new firmware image is validated, the new image is written to the device flash memory, and the router is automatically rebooted with the new firmware. The **System Information** section displays the latest firmware.

Changing the Language

To change the language:

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

STEP 2 In the **File Type** field, click the **Language File** button.

STEP 3 Click **Browse** to locate and select the language file.

STEP 4 Optionally, to restore the device configuration parameters to factory default vaues, select **Reset all configuration/settings to factory defaults**.

STEP 5 Click **Start Upgrade**.

Restarting the Cisco RV215W

To restart the router:

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

STEP 2 Click **Reboot**.

Restoring the Factory Defaults

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

To restore factory defaults to the router:

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

STEP 2 Click **Default**.

Running the Setup Wizard

To run the Setup Wizard:

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

STEP 2 Follow the online instructions.

A

Using Cisco QuickVPN

Overview

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

This appendix includes the following sections:

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

Before You Begin

The QuickVPN program only works with a router that is properly configured to accept a QuickVPN connection. You must perform the following steps:

STEP 1 Enable remote management. See **Configuring Basic Firewall Settings**.

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

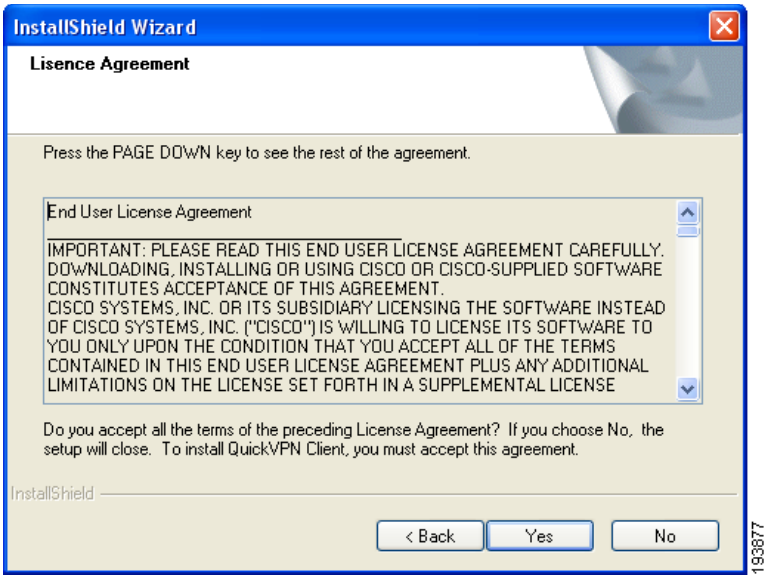
Installing the Cisco QuickVPN Software

Installing from the CD-ROM

STEP 1 Insert the Cisco RV215W CD-ROM into your CD-ROM drive. After the Setup Wizard begins, click the **Install QuickVPN** link.

The License Agreement window appears.

License Agreement



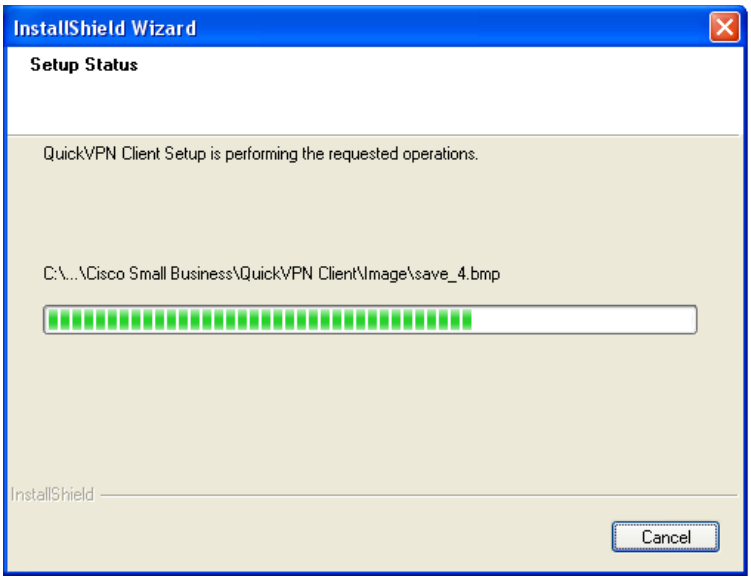
STEP 2 Click **Yes** to accept the agreement.

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

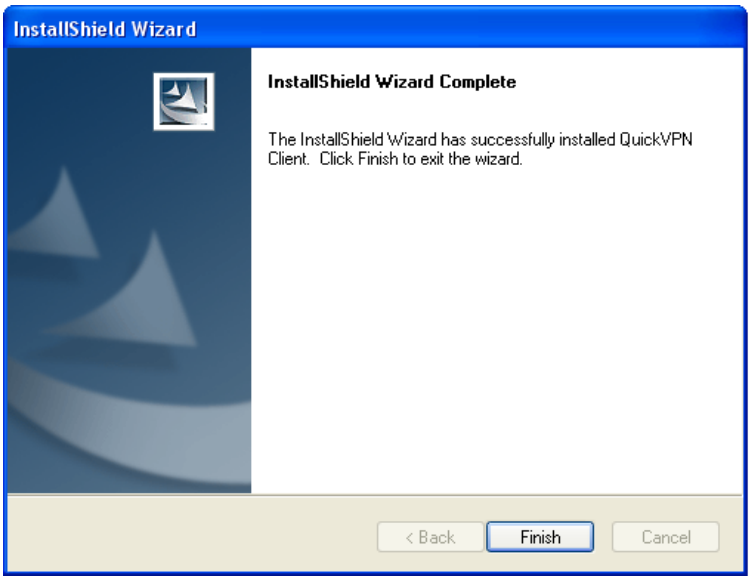
STEP 4 Click **Next**.

The Setup Wizard copies the files to the chosen location.

Copying Files



Finished Installing Files



STEP 5 Click **Finish** to complete the installation. Proceed to **"Using the Cisco QuickVPN Software," on page 146**.

Downloading and Installing from the Internet

STEP 1 In **Appendix B, "Where to Go From Here,"** go to the Software Downloads link.

STEP 2 Enter Cisco RV215W in the search box and find the **QuickVPN** software.

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

STEP 4 Double-click the .exe file, and follow the on-screen instructions.

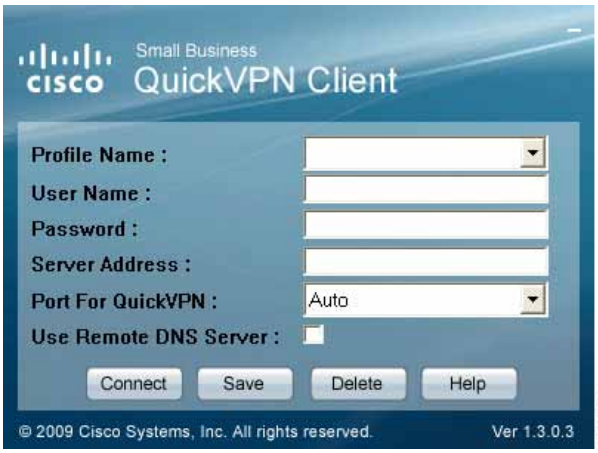
Using the Cisco QuickVPN Software

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

QuickVPN Desktop Icon

QuickVPN Tray Icon—
No Connection

The QuickVPN Login window appears.



STEP 2 In the **Profile Name** field, enter a name for your profile.

STEP 3 In the **User Name** and **Password** fields, enter the User Name and Password.

STEP 4 In the **Server Address** field, enter the IP address or domain name of the Cisco RV215W.

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.

QuickVPN Tray Icon—Connection

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.

B

Where to Go From Here

Support	
Cisco Support Community	www.cisco.com/go/smallbizsupport
Online Technical Support and Documentation (Login Required)	www.cisco.com/support
Phone Support Contacts	www.cisco.com/en/US/support/tsd_cisco_small_ business_support_ center_contacts.html
Software Downloads (Login Required)	Go to tools.cisco.com/support/downloads, and enter the model number in the Software Search box.

Product Documentation	
Wireless-N VPN Firewall	www.cisco.com/en/US/products/ps9923/tsd_products_support_series_home.html
Cisco Partner Central (Partner Login Required)	www.cisco.com/web/partners/sell/smb
Marketplace	www.cisco.com/go/marketplace