ADMINISTRATION GUIDE

Cisco RV130 Multifunction VPN Router

Cisco RV130W Wireless Multifunction VPN Router

Revised August 2014

1

Getting Started

The **Getting Started** page displays the most common configuration tasks on your device. Click the links on the Web page to go 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. For example, the device host name. See **Configuring Wired WAN Connections**.
Configure LAN Settings	Opens the **LAN Configuration** page to modify LAN parameters. For example, the management IP address. See **Configuring LAN Settings**.
Configure Wireless Settings	Open the **Basic Settings** page to manage the radio. See **Configuring Wireless Networks**.

Quick Access

Upgrade Router Firmware	Opens the **Firmware/Language Upgrade** page to update the device firmware or language pack. See **Upgrading Firmware or Changing the Language**.
Add VPN Clients	Opens the **PPTP Server** page to set up and manage VPN tunnels. See **Configuring PPTP**.
Configure Remote Management Access	Opens the **Basic Settings** page to enable the basic features of the device. See **Configuring Basic Firewall Settings**.

Device Status

System Summary	Displays the **System Summary** page that shows the state of the firmware, IPv4 and IPv6 configuration status, and the status of the wireless and the firewall on the device. 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 **IPsec VPN Server** page that lists the VPN managed by this device. See **Viewing Site-to-Site IPsec VPN Connection Status**.

Other Resources

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

Connecting to Your Wireless Network

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

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

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) that you chose for your network in the Setup Wizard.

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

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

STEP 4 Verify your wireless connection and save your settings.

2

Viewing Device Status

To ensure that data and statistics are frequently updated on Status pages, choose a refresh rate from the **Refresh Rate** drop-down list.

Viewing the Dashboard

Choose **Status** > **Dashboard** to view a snapshot of the configuration of your device. The Dashboard page displays information about your device's firmware version, CPU and memory utilization, error-logging settings, LAN, WAN, wireless, site-to-site IPsec VPN, and PPTP VPN server settings.

To modify the information displayed, click the **details** link to go to the configuration page for the section. For more information about managing the settings displayed on the Dashboard page, see:

- **Configuring Log Settings**
- **Configuring Basic Site-to-Site IPsec VPN**
- **Configuring LAN Settings**
- **Configuring Wired WAN Connections**
- **Configuring Basic Wireless Settings**

From the **Refresh Rate** drop-down list, choose the rate at which the latest statistics and parameter values are refreshed on the dashboard.

The Dashboard page also displays an interactive view of your device's back panel when you click **Show Panel View**. Mouse-over each port to view port connection information.

Viewing the System Summary

Choose **Status** > **System Summary** to view details of your device properties, network settings across IP address modes, firewall, wireless and VPN settings. Click **Refresh** to see the latest information.

Click the underlined link to go to the related configuration window. For example, to modify the LAN IP address, click **LAN IP**. The LAN Configuration window is displayed.

The **System Summary** page displays information in the following sections:

System Information

- **Firmware Version—**Current software version that 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 checks 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—**Length of time that 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. To release the current IP address and obtain a new one, click **Release** or **Renew**.
- Gateway—IP address of the gateway to which the device 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 device is connected (for example, the cable modem).
- Prefix Delegation—Prefix returned from the device at the ISP, which is provided to IPv6 addresses on the device.
- **DNS 1—**IP address of the primary DNS server.
- **DNS 2—**IP address of the secondary DNS server.

Wireless Summary

Displays the public name and security settings for your wireless networks configured on the Wireless > Basic Settings page. For more information, see **Configuring Basic Wireless Settings**.

Firewall Setting Status

Displays DoS, WAN request and remote management settings configured on the Firewall > Basic Settings page. For more information, see **Configuring Basic Firewall Settings**.

VPN Setting Status

Displays available IPsec and PPTP VPN connections, and the connected users for each VPN type.

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

For more information on configuring VPN server connections and user accounts, see **Configuring Basic Site-to-Site IPsec VPN** and **Configuring PPTP**.

Viewing Active TCP/IP Services

Choose **Status > Active TCP/IP Services** to view IPv4 and IPv6 TCP/IP connections that are active on your device. The **Active Service List** section for IPv4 and IPv6 displays the protocols and the services that are active on the device.

Viewing Wireless Statistics

Choose **Status > Wireless Statistics** to view wireless statistical data for the device radio. In the **Refresh Rate** field, choose the rate at which you want the latest statistics to be displayed.

To show the bytes in kilobytes (KB) and the numerical data in rounded-up values, check the **Show Simplified Statistic Data check** box 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**. The counters are reset when the device is rebooted.

Viewing Captive Portal Status

Choose **Status > Captive Portal** to view information about the connected Captive Portal users. For more information about configuring Captive Portals on your device, see **Configuring Captive Portal**.

Viewing Site-to-Site IPsec VPN Connection Status

Choose **Status > Site-to-Site IPsec VPN** to view the connection status of active site-to-site IPsec VPN policies on the device. For information on configuring VPN policies, see **Configuring Basic Site-to-Site IPsec VPN**.

To change the rate at which latest and real-time connection status is displayed, choose a refresh rate from the **Refresh Rate** drop-down list.

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 the **Show Simplified Statistic Data** box and click **Save**.

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

Viewing the IPsec VPN Server Status

Choose **Status > IPsec VPN Server** to view a list of your IPsec VPN connections and the duration of the connection. For more information about configuring IPsec VPN connections, see **Configuring IPsec VPN Server**.

Viewing PPTP Server

Choose **Status > PPTP Server** to view a list of your PPTP VPN connections, the duration of the connection, and the actions you can perfom on this connection. For more information about configuring PPTP VPN connections, see **Configuring PPTP**.

Viewing Logs

Choose **Status > View Logs**. Click **Refresh Logs**, to display latest log entries.

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, checking the **Error** check box 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**—Messages about events such as a system crash.
- **Alert**—Messages about conditions that require immediate corrective action.
- **Critical**—Messages for when the system is in a critical condition.

- **Error**—Messages about conditions that are not critical but require corrective action.
- **Warning**—System warnings.
- **Notification**—Messages about normal but significant conditions that may require attention.
- **Informational**—Messages about device information.
- **Debugging**—Detailed information about an event.

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

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

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

To move between log pages, use the page navigation buttons .

Viewing Connected Devices

The **Connected Devices** page displays information about the active client devices connected to your router. 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) devices connected to the router.

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

IPv6 NDP Table displays all IPv6 Neighbor Discovery Protocol (NDP) devices connected to the device’s local link.

Viewing Port Statistics

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

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

To refresh the page at regular intervals, choose a refresh rate from the **Refresh Rate** drop-down list.

To show the bytes in kilobytes (KB) and the numerical data in rounded-up form, check the **Show Simplified Statistic Data** box 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 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**—The length of time that link has been up.
- **Current Session Usage**—Volume of data being received (Rx) and transmitted (Tx) on the mobile link.
- **Monthly Usage**—Monthly data download and bandwidth usage.
- **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.
- **Card Status**—Status of the data card.

3

Configuring Networking

Configuring 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 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 DHCP WAN settings:

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

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

STEP 3 From the **DNS Server Source** drop-down list, choose one of the following ways to set the DNS server address:

- If you already have DNS server addresses from your ISP, choose **Use these DNS Servers**, and enter the primary and secondary addresses.
- If you do not have DNS server addresses from your ISP, choose **Get Dynamically from ISP**.
- To use the DNS servers provided by OpenDNS (208.67.222.222, 208.67.220.220) to resolve your web addresses, choose **Use OpenDNS**.

STEP 4 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 WAN port.
Subnet mask	Subnet mask of the WAN port.
DNS Server Source	The DNS server address. If you already have DNS server addresses from your ISP, choose **Use these DNS Servers**, and enter the primary and secondary addresses in the **Static DNS 1** and **Static DNS 2** fields. To use the DNS servers provided by OpenDNS (208.67.222.222, 208.67.220.220) to resolve your web addresses, choose **Use OpenDNS**.
Default Gateway	IP address of the default gateway.

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 Select a PPPoE profile or click **Configure Profile** to create a new profile.

STEP 4 On the PPPoE Profiles page, enter the following information (you might need to contact your ISP to obtain your PPPoE login information):

Profile Name	A unique name for the PPPoE profile.
Username	The username assigned by the ISP.
Password	The password assigned by the ISP.
DNS Server Source	The DNS server address. If you already have DNS server addresses from your ISP, choose **Use these DNS Servers**, and enter the primary and secondary addresses in the **Static DNS 1** and **Static DNS 2** fields. To get DNS server addresses from your ISP, choose **Get Dynamically from ISP**. To use the DNS servers provided by OpenDNS (208.67.222.222, 208.67.220.220) to resolve your web addresses, choose **Use OpenDNS**.
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 5 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 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.
Service Name	Enter a name for the new PPTP service.
MPPE Encryption	Check the **Enable** check box to enable Microsoft Point-to-Point Encryption for the PPTP connection.

DNS Server Source	The DNS server address. If you already have DNS server addresses from your ISP, choose **Use these DNS Servers**, and enter the primary and secondary addresses in the **Static DNS 1** and **Static DNS 2** fields. To get DNS server addresses from your ISP, choose **Get Dynamically from ISP**. To use the DNS servers provided by OpenDNS (208.67.222.222, 208.67.220.220) to resolve your web addresses, choose **Use OpenDNS**.

STEP 4 Click **Save**.

Configuring L2TP

To configure 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	The IP address of the WAN port.
Subnet mask	The subnet mask of the WAN port.
Default Gateway	The IP address of the default gateway.
L2TP Server	The IP address of the L2TP server.
Version	The L2TP version that you want to use. If you select version 3, enter the vendor ID, and the virtual circuit ID.
Cookie Length	The size of the cookie in the L2TP v3 data packet, which identifies the L2TP session.

Vendor ID	The vendor ID contained in the AVP encoding format for L2TP. To use the IETF-adopted attribute values in the AVP, select **Standard**. To implement Cisco's L2TP extensions and private attribute values, select **Cisco**.
Virtual Circuit ID	The identifier for the Layer 2 circuit over which L2TP data packets are carried. This information is required if you selected Cisco as the **Vendor ID** for L2TP v3.
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.

Service Name	Enter a name for the new L2TP service.
MPPE Encryption	Check **Enable** to enable Microsoft Point-to-Point Encryption for the L2TP connection.
DNS Server Source	The DNS server address. If you already have DNS server addresses from your ISP, choose **Use these DNS Servers**, and enter the primary and secondary addresses in the **Static DNS 1** and **Static DNS 2** fields. To get DNS server addresses from your ISP, choose **Get Dynamically from ISP**. To use the DNS servers provided by OpenDNS (208.67.222.222, 208.67.220.220) to resolve your web addresses, choose **Use OpenDNS**.

STEP 4 Click **Save**.

Configuring Optional Network Settings

To configure optional settings:

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

MTU	Maximum transmission unit (MTU) is 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 default MTU size is 1500 bytes. If your ISP requires a custom MTU setting, choose **Manual** and enter the MTU size.
Size	The custom MTU size. The standard MTU value for Ethernet networks is usually 1500 bytes. For PPPoE connections, the value is 1492 bytes.

Untagged VLAN	Check the box to enable VLAN tagging. When enabled (the default), all traffic is tagged with a VLAN ID. By default, all traffic on the device uses VLAN 1, the default untagged VLAN. All traffic is untagged until you disable the untagged VLAN, change the untagged traffic VLAN ID, or change the VLAN ID.
Untagged VLAN ID	A number between 1 and 4094 for the untagged VLAN ID. The default is 1. Traffic on the VLAN that you specify in this field is not tagged with a VLAN ID when forwarded to the network. VLAN 1 is the default untagged VLAN.
AP Management VLAN	The VLAN associated with the IP address you use to access the device when it is configured as an access point. If you create additional VLANs, for security reasons, choose a value that corresponds with the VLAN configured on other switches in the network. You may need to change the management VLAN to limit access to Device Manager.

STEP 2 Click **Save**.

Configuring a Mobile Network

Choose **Networking > WAN > Mobile Network** to configure to configure the device to connect to a Mobile Broadband USB modem that is connected to its USB interface.

Configuring Global Mobile Network Settings

To configure global settings for supported USB devices:

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**, set a **Connect on Demand** time or select **Keep Alive**. **Connect on Demand** terminates the Internet connection after it is inactive for the period of time specified in the **Max Idle Time** field.

  If your Internet connection is terminated due to inactivity, the modem automatically reestablishes 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. Select **Keep Alive** to keep the connection active 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 your mobile card is **Connected**.

Configuring Mobile Network Settings Manually

To change mobile network parameters in the **Mobile Network Setup** area, click the **Manual** radio button. The device automatically detects supported modems and lists the appropriate configuration parameters. To override global parameters, select **Manual**.

STEP 1 Enter information in 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.
Username **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. You can modify the SIM PIN in either Auto or Manual mode.
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
Server 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. **Auto** chooses a signal based on the area service signal. **4G only** searches for only 4G signals. **3G only** searches for only 3G signals.

STEP 2 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 given threshold, sends a notification.

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

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

STEP 2 Select the **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, see **Configuring Log E-Mailing**.

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 Ethernet and mobile network links are available, only one connection can be used to establish a WAN link, at a time. When one WAN connection fails, the device attempts to establish a connection on another interface. This feature is called Failover. When the primary WAN connection is restored, it reverts to the original path and ends the backup connection. This feature is called Recovery.

STEP 1 Choose **Networking > WAN > Failover & Recovery**, to display the Failover & Recovery window.

STEP 2 Select **Enable Failover to 3G WAN** to enable the mobile network link and set it to failover from the Ethernet link. When the Ethernet WAN link is not active, the device attempts to enable the mobile network link on the USB interface. (If failover is not enabled, the mobile network link is always disabled.)

STEP 3 Select **Enable Recovery back to Ethernet WAN** to enable the link to return to the Ethernet link, dropping the mobile network link. The Connect Mode accessed through **WAN > Mobile Network** must be set to **Auto** to use Ethernet WAN connection recovery.

STEP 4 In the **Failover Check Interval** field, enter the frequency (in seconds) with which the device must attempt to detect the physical connection or presence of traffic on the mobile network link. If the link is idle, the device attempts to ping a destination at this interval. If there is no reply to the ping packet, the device assumes the link is down and retries the Ethernet WAN interface.

STEP 5 In the **Recovery Check Interval** field, enter the frequency (in seconds) with which the device must attempt to detect the physical connection or presence of traffic on the Ethernet WAN link. If the link is idle, the device attempts to ping a destination at the interval. If there is a reply to the ping packet, the device assumes the link is up and attempts to disable the mobile network link and enable the Ethernet WAN link.

STEP 6 Click **Switch back to Ethernet immediately when Ethernet is available** or click **Switch back to Ethernet in a specific time range** and enter the start and end time for the range.

STEP 7 In the **Connection Validation Site** field, choose the site from which to perform failover validation. Use the next hop gateway (by default the device pings the default gateway) or choose a custom site and enter the site IPv4 or IPv6 address.

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

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.

Configuring 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 the device sends to DHCP clients.

If your device is connected to a modem or to another device that has a configured network on the same subnet (192.168.1.x), it 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 router.

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. Make sure 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 IP address of your device, 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 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 other 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 that the DHCP pool is set to the default parameters, static IP addresses from 192.168.1.2 to 192.168.1.99 in the IP address pool can be used to prevent 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 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 the following 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.
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 your router to assign a specific IP address to a client device with a specific MAC address.

To configure static DHCP:

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

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

STEP 3 Click **Add Row**.

STEP 4 Enter the following information:

Description	Description of the client.
IP Address	IP address you want assigned to the client 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 client device is connected to the network. The DHCP server assigns the reserved IP address when the client device using the corresponding MAC address requests an IP address.
MAC Address	MAC address of the client 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 Client**.

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

Your 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 Enter the following information:

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.
Jumbo Frame	Check to enable jumbo frames on the device and send frames within the LAN containing up to 9,000 bytes of data per frame. A standard Ethernet frame contains 1,500 bytes of data.
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**.

Configuring Link Aggregation

Use the Link Aggregation page to group multiple Ethernet links into a single logical channel. Link aggregation groups improve the cost effectiveness of your device by increasing cumulative bandwidth without requiring hardware upgrades, and facilitates easy rerouting in case of a single port or cable failure.

To assign ports to link aggregation group:

STEP 1 Choose **Networking > LAN > Link Aggregation**. The **Port Status** section displays the mode associated with each port on the device and the status.

STEP 2 In the **Link Aggregation Setting Table** section, check the check box for each port to include it in the group.

STEP 3 Click **Save**.

Cloning the MAC Address

Sometimes, you might 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 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, you can clone the MAC address of the WAN port to be the same as your computer MAC address.

To configure a MAC address clone:

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

STEP 2 In the **MAC Address Clone** field, check **Enable**.

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

Use the Routing page to configure the operating mode and other routing options for your device.

Configuring the Operating Mode

To configure the operating mode:

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

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

Gateway	To set the device to act as a gateway. (Recommended) Keep this default setting if the device is hosting your network connection to the Internet and is performing routing functions.
Router	(For advanced users only) 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.

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 Inter VLAN Routing

To allow an end station in one VLAN to communicate with an end station in another VLAN, check the **Inter VLAN Routing Enable** check box.

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** page.

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 The **DDNS Service Table** section lists the DDNS services that you can enable on the device.

STEP 3 Check the check box for the service you want to enable and click **Edit**.

STEP 4 Check the **Enable** check box for the service.

STEP 5 Configure this information:

Username/E-mail Address	The username of the DDNS account or the e-mail address that you used to create the DDNS account.
Password	Password of the DDNS account.
Host / Domain Name	Hostname of the DDNS server or the name of the domain that is used to access the network
Internet IP Address	(Read-only) Internet IP address of your device.
Status	(Read-only) Indicates that the DDNS update has completed successfully or the account update information sent to the DDNS server failed.

STEP 6 Click **Test Configuration**, to test the DDNS configuration.

STEP 7 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	To use IPv4 on the LAN and WAN ports.
LAN:IPv6, WAN:IPv4	To use IPv6 on the LAN ports and IPv4 on the WAN ports.
LAN:IPv6, WAN:IPv6	To use IPv6 on the LAN and WAN ports.
LAN:IPv4+IPv6, WAN:IPv4	To use IPv4 and IPv6 on the LAN ports and IPv4 on the WAN ports.
LAN:IPv4+IPV6, WAN:IPv4+IPv6	To use IPv4 and IPv6 on both the LAN and WAN ports.
LAN:IPv4, WAN:IPv6	To 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 your 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 SLAAC

To self-assign an address based on the IPv6 prefix, configure the device to use use Stateless Address Auto-Configuration (SLAAC) for IPv6 client address assignment.

To use SLAAC:

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

STEP 2 In the **WAN Connection Type** field, select **SLAAC**. For stateless DHCP, it is not necessary to have a DHCPv6 server available at the ISP. Instead, an ICMPv6 discover message originating from your device is used for auto-configuration.

STEP 3 Click **Save**.

Configuring DHCPv6

If your ISP provides you with a dynamically assigned address, configure the device to be 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**. The gateway connects to the ISP's DHCPv6 server for a leased address.

STEP 3 To automate assigning prefixes to your device (the DHCP client), select the **Prefix Delegation Enable** radio button.

STEP 4 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**.

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	Maximum transmission unit is 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 your 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**
- **6RD** (Rapid Deployment)
- ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) - Choose **Auto** or **Manual**.

STEP 4 For 6RD Tunneling, choose **Auto** or **Manual**. If you choose **Manual**, enter the following information:

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

STEP 5 For ISATAP Tunneling, choose **Auto** or **Manual**. If you choose **Manual**, enter the following information:

- **IPv6 Prefix**
- **IPv6 Prefix 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 the **Enable** box.

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 transmission 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**.

4

Configuring Wireless Networks

Wireless Security

Wireless networks are convenient and easy to install. 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 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 prevent 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. We recommend 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.

Wireless Networks on Your Device

Your device 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
VLAN	1	1	1	1
Wireless Isolation with SSID	Disabled	Disabled	Disabled	Disabled
WMM	Enabled	Enabled	Enabled	Enabled

SSID Name	ciscosb1	ciscosb2	ciscosb3	ciscosb4
WPS Hardware Button	Enabled	Disabled	Disabled	Disabled

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

Configuring Basic Wireless Settings

Choose **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 the **Enable** box 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	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 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, which 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 Wireless Network Settings**).

STEP 9 Click **Save**.

Editing Wireless Network Settings

The **Wireless Table** on the **Basic Settings** page 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 that you want to configure.

STEP 2 Click **Edit**.

STEP 3 Configure the following 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.
Security Mode	See **Configuring the Security Mode**.
MAC Filter	See **Configuring MAC Filtering**.
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.
Max Associated Clients	The maximum number of clients that can connect to the selected wireless network. Enter a number between 1 and 64.
WPS	Check this box to map the device WPS button on the front panel to this network.
Portal Profile	See **Configuring Captive Portal**.

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 Choose **Wireless** > **Basic Settings**. In the **Wireless Table**, check the box for the network you want to configure.

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

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

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

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

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

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

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

- **10/64-bit(10 hex digits)—**Provides a 40-bit key.
- **26/128-bit(26 hex digits)**—Provides a a 104-bit key, which offers stronger encryption, making the key more difficult to decipher. 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. 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** filed, 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 during the day, when access to the network is allowed.

STEP 5 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	Enabling WMM No Acknowledgement can result in more efficient throughput, but higher error rates in a noisy Radio Frequency (RF) environment. By default, this 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 device 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 device 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 device supports N speeds. Other options are 1-2 Mbps, for use with older wireless technology, and All, when the device can transmit at all wireless rates. The Basic Rate is not the actual rate of data transmission. If you want to specify the device 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 device automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the device 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 device automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the device and a wireless client. The default is Auto.

CTS Protection Mode	The device automatically uses 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 device in an environment with heavy 802.11b traffic. This function boosts the device's ability to catch all Wireless-N and Wireless-G transmissions but will severely decrease performance. The default is Auto.
Beacon Interval	The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the device 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 device 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**.

Detecting Rogue Access Points

A rogue access point is an access point (AP) that has been installed on a secure network without authorization from a system administrator. Rogue APs pose a security threat because anyone with access to the premises can install a wireless AP that can allow unauthorized parties to access the network.

Use the Rogue AP Detection page to enable your device to display information about all APs detected by the device in the vicinity of the network. If the access point listed as a rogue is actually a legitimate access point, you can add it to the **Authorized AP Table**. Select a refresh rate to ensure that the Rogue AP Detection page always displays the latest information.

To enable Rogue AP detection:

STEP 1 Choose **Wireless > Rogue AP**.

STEP 2 Click the **Rogue AP Detection On** radio button.

STEP 3 Click **Save**.

To authorize detected access points:

STEP 1 In **Rogue AP Detected Table**, check the box for the access point that you want to authorize.

STEP 2 Click **Authorize**.

To add an access point to the Authorized AP table:

STEP 1 Click **Add Row**.

STEP 2 Enter the MAC address of the access point that you want to authorize.

STEP 3 Enter the SSID or the name that identifies the wireless network.

STEP 4 Choose the security mode associated with the access point.

STEP 5 Choose **TKIP** (Temporal Key Integrity Protocol) or **CCMP** (Counter Cipher Mode Protocol) as the encryption algorithm associated with the access point.

STEP 6 Choose **RADIUS** server or **PSK** (Pre-Shared Key) to authenticate the access point.

STEP 7 Select the wireless network mode that the access point uses.

STEP 8 Choose the radio frequency that the access point uses.

STEP 9 Click **Save**.

Importing Authorized AP Lists

You can import a list of authorized access points using a CSV file. Use the following values as a reference when you create the CSV file.

Field	Values
Security	• 0 – Open • 1 – WEP • 2 – WPA-Personal • 3 – WPA-Enterprise • 4 – WPA2-Personal • 5 – WPA2-Enterprise
Network Mode	• 0 – B Only • 1 – G Only • 2 – N Only • 3 – BG-Mixed • 4 – GN-Mixed • 5 – BGN-Mixed
Channel	• 0 – Auto • 1 – 2.412 • 2 – 2.417 • 3 – 2.422 • 4 – 2.427 • 5 – 2.432 • 6 – 2.437 • 7 – 2.442 • 8 – 2.447 • 9 – 2.452 • 10 – 2.457 • 11 – 2.462

Field	Values
Encryption	• 2 – TKIP • 4 – CCMP
Authentication	• 2 – PSK • 1 – RADIUS

Ensure that the content in the CSV file is arranged as shown in the following example:

BSSID	Security	Encryption	Authentication	Wireless Network	Channel	SSID
00:1C:10:CE:44:48	4	2	2	3	1	Auth_Guest

To import a list of authorized APs:

STEP 1 Click **Merge** to add the list of access points that you want to import, to the access points displayed in **Authorized AP Table**. Click **Replace** to replace the APs in the table with the APs in the list that you want to import.

STEP 2 Click **Browse** to locate the file that you want to import.

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 device 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).

You can configure WDS in Bridge mode where one AP acts as the common link between multiple APs or in Repeater mode where one AP connects two APs without a wired connection to the LAN, by repeating signals using the wireless connection.

WDS is supported on one SSID only.

To configure WDS in Bridge mode:

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

STEP 2 To enable WDS, check the **WDS** check box.

STEP 3 Select the **WDS Bridge** radio button.

STEP 4 In the **Remote Wireless Bridge's MAC Address** section, enter the MAC addresses of up to four access points to use as bridges in the **MAC 1**, **MAC 2**, **MAC 3**,and **MAC 4** fields.

STEP 5 Click **Save**.

To configure WDS in Repeater mode:

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

STEP 2 Check the **WDS** check box.

STEP 3 Choose the repeater mode. If you select **Allow wireless signal to be repeated by a repeater**, 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 If you select **Repeat wireless signal of a remote access point**:

- Enter the MAC address of a wireless access point in the **MAC** field.
- Click **Show Available Networks** to display the **Available Networks Table.** Click **Connect** to add the MAC address of the selected access point to the MAC field.

STEP 5 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 Click **Edit** to change the wireless network on which to enable WPS

STEP 3 Configure the WPS on client devices in one of the following three ways:

- Click or press the WPS button on the client device and click the WPS icon on this page.
- Enter the WPS PIN number of the client and click **Register**.
- A client device requires a PIN number from this 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.

Configuring Captive Portal

Use the Captive Portal feature to provide controlled, authenticated access to the Internet and your network resources, without compromising security. A captive portal displays a special web page to authenticate clients before they can use the Internet. You can configure Captive Portal verification to allow access for both guest and authenticated network users.

Configure Captive Portal instances for each virtual wireless network on your device by associating it with a portal profile.

Creating Captive Portal Profiles

To create a captive portal profile:

STEP 1 Choose **Wireless > Captive Portal > Portal Profile.** In the **Portal Profile Table** section, click **Add Row**. To modify the portal profile provided on the device, check the **Default_Portal_Profile** box and click **Edit**.

STEP 2 Enter a name for your Captive Portal profile.

STEP 3 Choose if you want to use the profile to authenticate guest users or users on your network.

STEP 4 To redirect users to a URL after authentication, enable **Auto Redirect URL**, and enter a fully qualified domain name or IP address in the **Redirect URL** field. For example, include http:// in the URL.

STEP 5 In the **Session Timeout** field, specify the number of minutes that the device will keep an authentication session open with the associated wireless client. The default timeout is 60 minutes.

STEP 6 Select a font color for the text that you want to display on the page.

STEP 7 Specify the text that you want to display, such as the name of your organization, the label text for username and password fields, and the label on the Login button.

STEP 8 Enter standard Copyright text associated with your company.

STEP 9 In the **Error 1** and **Error 2** fields, enter the error messages that you want to display to clients when login fails and when the maximum number of connections is exceeded.

STEP 10 To use a check box to allow users to accept terms of use before they continue, enable **Agreement.** The text in the **Agreement Text** field will be displayed as the label for the checkbox.

STEP 11 Enter the acceptance terms that you want to display to users in the **Acceptance Use Policy** field.

STEP 12 In the **Upload Files** section, choose files to upload your company logo and background files in keeping with your company’s branding guidelines. Save your profile.

To preview this profile, choose **Captive Portal > Portal Page Preview**, and select the profile from the **Portal Profile** drop-down list.

Configuring Captive Portal Instances

To configure a captive portal instance for your device:

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

STEP 2 In the **Wireless Table** section, check the **Enable** box for the SSID for which you want to configure a captive portal. Click **Edit**.

STEP 3 Select a portal profile for the SSID.

You can create up to four captive portals using the SSIDs for your device. To create a new portal profile, select **Create a new Portal Profile** from the drop-down list. Choose Default_Portal_Profile to use the portal profile provided on your device.

STEP 4 Check the **Enable** box to enable the captive portal for the SSID.

STEP 5 Save your captive portal instances.

Creating Captive Portal User Accounts

To create a captive portal user account:

STEP 1 Choose **Wireless > Captive Portal > User Accounts**.

STEP 2 Click **Add Row**.

STEP 3 Enter a username and password. Reenter the password to verify it.

We recommended 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.

STEP 4 In the **Access Time (Minutes)** field, specify the duration after which the authentication session will timeout.

STEP 5 To import usernames and passwords from a CSV file, click **Import**. The **Administration > Users** page is displayed. In the **Import Username and Password** section, click **Browse** to locate the file, and click **Import**. See **Importing User Accounts** for more information.

STEP 6 Save your user accounts.

Configuring Device Mode

You can configure your device to work in the following modes:

- **Router**—To act as a wireless router.
- **AP (access point)**—To provide wireless connections to clients and extend Wi-Fi capability to an existing wired network. All LAN ports are disabled when the device works as an access point.

  Ensure that you configure the AP management VLAN information on the **Networking > WAN > WAN Configuration** page. For more information, see **Configuring Optional Network Settings**.

To configure the device mode:

STEP 1 Choose **Wireless > Device Mode**, and select the mode in which you want to run your device.

STEP 2 Click **Save**.

5

Configuring the Firewall

Firewall Features

You can secure your network by creating and applying rules that the 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 that the router should allow or block. For example, web browsing, VoIP, other standard services and custom services that you define.
- 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 specific groups of PCs on your network from being accessed by the WAN or public DMZ network.

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

If you want to allow incoming traffic, you must make the router's WAN port IP address known to the public. This is called “exposing your host.” How you make your address known depends on how the WAN ports are configured; for the 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:

IP Address Spoofing Protection	To protect your network against IP address spoofing, check the **Enable** check box.
DoS Protection	Check **Enable** to enable Denial of Service protection.
Block WAN Request	Blocks ping requests to the device from the WAN.
LAN/VPN 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.
SIP ALG	To allow Session Initiation Protocol (SIP) traffic to traverse the firewall, check the **SIP ALG** check box. The device supports a maximum of 256 sessions.
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.

STEP 3 Click **Save**.

Configuring Remote Management

You can enable remote management so that 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, it is highly recommended that you change the administrator and any guest passwords before continuing.

Configuring Universal Plug and Play

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

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 In the **Scheduled Days** section, choose if you want to apply the schedule to All days or Specific Days. If you choose **Specific Days**, check the box next to the days that you want to include in the schedule.

STEP 5 In the **Scheduled Time of Day** section, choose the time when you want the schedule to apply. 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.

NOTE Internet access policies override access rules, when both are configured on the device.

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

STEP 5 From the **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 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 7 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 8 Check the **Rule Status Enable** check box, to enable the new access rule.

STEP 9 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 Check the **Status Enable** check box.

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 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 Domain Name & Keyword** table, click **Add Row**.

b. From the **Type** drop-down menu, choose how to block a website (by specifying the domain name 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 One-to-One Network Address Translation (NAT)

Use the One-to-one NAT page to map local IP addresses behind your firewall to global IP addresses. One-to-one NAT is a way to make systems configured with private IP addresses, which are behind a firewall, appear to have public IP addresses.

To add a One-to-One NAT rule:

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

STEP 2 Click **Add Row**.

STEP 3 In the **Private Range Begin** field, enter the starting IP address in the private (LAN) IP address range.

STEP 4 In the **Public Range Begin** field, enter the starting IP address in the public (WAN) IP address range.

STEP 5 In the **Range Length**, enter the number of public IP addresses that should be mapped to private addresses.

STEP 6 In the **Service** field, choose the service for which the rule applies. Services for one-to-one NAT allow you to configure the service to be accepted by the private IP (LAN) address when traffic is sent to the corresponding public IP address. Configured services on private IP addresses in the range are accepted when traffic is available on the corresponding public IP address.

STEP 7 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, when external devices connect to them, they receive data on a specific port or range of ports in order to function properly. The router must send all incoming data for that application only on the required port or range of ports.

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

Configuring Single Port Forwarding

To add a single port forwarding rule:

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

6

Configuring VPN

VPN Tunnel Types

You can configure VPN on your device to provide you a secure communication channel or a tunnel between:

- Two gateway routers
- A remote client device and a gateway router

Configuring Basic Site-to-Site IPsec VPN

Your device supports site-to-site IPsec VPN for a single gateway-to-gateway VPN tunnel. After configuring these basic VPN settings, you can connect securely to another VPN-enabled router. For example, you can configure your device at a branch site to connect to a router that connects site-to-site VPN tunnels at the corporate site, so that the branch site has secure access to the corporate network.

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

STEP 1 Choose **VPN >** Site-to-Site IPsec VPN **> Basic VPN Setup**.

STEP 2 In the New 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 if the router to which your device will connect will be identified by its IP address or by a fully qualified domain name. For example, an IP address such as 192.168.1.1 or 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.
- Local WAN (Internet) IP Address—Enter the public IP address or domain name of your device.

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

- **Remote LAN (Local Network) IP Address**—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**—The private network (LAN) subnet mask of the remote endpoint.
- **Local LAN (Local Network) IP Address**—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**—The private network (LAN) subnet mask of the local network.

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 causes a 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

Click **View Default Settings** to view the default values used in the basic VPN settings. These values are proposed by the VPN consortium and assume that you are using a pre-shared key, or password that is known to both your device and the remote endpoint.

Configuring Site-to-Site IPsec VPN Advanced Parameters

Advanced VPN parameters such as IKE and other VPN policies control how the device initiates and receives VPN connections.

To configure advanced VPN parameters, choose **VPN > Site-to-Site IPsec VPN > Advanced VPN Setup**.

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 to be used when exchanging data with the remote router over the IPsec VPN connection. For example, you can create IKE policies to define parameters for peer authentication and encryption algorithms. Ensure that the encryption, authentication, and key-group parameters in your VPN policy. are compatible with settings at the remote router.

To add an IKE policy**:**

STEP 1 On the **Advanced VPN Setup** page, click **Add Row**.

STEP 2 Enter a unique name for the IKE policy to identify and manage the policy easily.

STEP 3 In the **Exchange Mode** field, choose one of the following modes for the policy:

- **Main**—Negotiates the tunnel with higher security, but is slower.
- **Aggressive**—Establishes a faster connection, but with lowered security.

STEP 4 In the **Local Identifier** and **Remote Identifier** fields, indicate if you want to identify your device and the remote router by their real IP address or their public IP address. If you select IP address, enter the real IP address of your device and the remote router.

STEP 5 In the **IKE SA Parameters** section, configure parameters to define the strength and mode for negotiating Security Association (SA) between your device and the remote router:

a. In the **Encryption Algorithm** field, choose the algorithm to encrypt data.

b. In the **Authentication Algorithm** field, specify the authentication algorithm for the VPN header. Ensure that the authentication algorithm is configured identically on both sides of the VPN tunnel.

c. In the **Pre-Shared Key** field, enter the key or password. Ensure that the password does not contain double-quotes (“).

d. In the **Diffie-Hellman (DH) Group** field, specify the DH Group algorithm used when exchanging a pre-shared key. 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.

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

f. To enable the **Dead Peer Detection** feature, check the **Enable** box. Dead Peer Detection (DPD) is used to detect if the peer is alive. If the peer is detected as dead, the device deletes the IPsec and IKE Security Association. If you enable this feature, also enter these settings:

- **DPD Delay—**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—**The maximum time that the device should wait to receive a response to the DPD message before considering the peer to be dead.

STEP 6 Click Save.

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

Managing VPN Policies

NOTE Before you create an Auto VPN Policy, ensure that you create the IKE policy based on which you want to create the auto VPN policy.

To manage VPN policies:

STEP 1 Choose **VPN > Site-to-Site IPsec VPN > Advanced VPN Setup**. Click **Add Row**.

STEP 2 In the **Add / Edit VPN Policy Configuration** section:

a. In the **Policy Name** field, enter a unique name to identify the policy.

b. In the **Policy Type** field, choose one of the following options:

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

c. **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 IP address or the FQDN.

STEP 3 In the **Local Traffic Selection** and **Remote Traffic Selection** sections:

- In **the Local IP and Remote IP** fields, indicate how many endpoints will be part of the VPN policy:
  - **Single**—Limits the policy to one host. Enter the IP address of the host that will be part of the VPN in the **IP Address** field.
  - **Subnet**—Allows an entire subnet to connect to the VPN. Enter the network address in the **IP Address** field, and enter the subnet mask in the **Subnet Mask** field. Enter the subnet's network IP address in the **IP Address** field. Enter the subnet mask, such as 255.255.255.0, in the **Subnet Mask** field. The field automatically displays the default subnet address based on the IP address.

Note: Do not use 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, avoid:

Local Traffic Selector: 192.168.1.0/24

Remote Traffic Selector: 192.168.0.0/16

STEP 4 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. Security Parameter Index (SPI) identifies the Security Association of the incoming and outgoing traffic streams.
- **Manual Encryption Algorithm**—Select the algorithm used to encrypt the data.
- **Key-In, Key-Out**—Enter the encryption key of the inbound and outbound 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

- **Manual Integrity Algorithm**—Select the algorithm used to verify the integrity of the data.
- **Key-In, Key Out**—Enter the integrity key (for ESP with Integrity-mode) for the inbound and outbound policy. The length of the key depends on the algorithm chosen:
  - MD5—16 characters
  - SHA-1—20 characters
  - SHA2-256—32 characters

STEP 5 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, 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.
- DH Group**—**Specify the DH Group algorithm used when exchanging a pre-shared key. 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.
- **Select IKE Policy—**Choose the IKE policy that will define the characteristics of the SA negotiation.

STEP 6 Click **Save**.

Configuring IPsec VPN Server

Using IPsec VPN enables secure remote access to corporate resources by establishing an encrypted tunnel across the Internet. Your device supports the following IPsec VPN clients:

- TheGreenBow
- ShrewSoft

Configuring the IPsec VPN Server

To configure the IPsec VPN server:

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

STEP 2 Check the **Server Enable** check box.

STEP 3 In the **Phase 1** section, configure settings to authenticate the two VPN endpoints to each other and negotiate the IKE Security Association (SA) so that a secure channel is set up for negotiating SAs in Phase 2.

a. In the **Pre-Shared Key** field, enter the pre-shared key or password that will be exchanged between your device and the remote endpoint. The password must be between 8 and 49 characters.

b. In the **Exchange Mode** field, choose one of the following modes for the IPsec VPN connection:

   - **Main**—Negotiate the tunnel with higher security, but is slower.
   - **Aggressive**—Establish a faster connection, but with lowered security.

c. Choose the **Encryption Algorithm** to encrypt data and choose the **Authentication Algorithm** for the VPN header. Ensure that the authentication algorithm is configured identically on both your device and the remote endpoint.

d. In the **Diffie-Hellman (DH) Group** field, specify the Diffie-Hellman Group algorithm used when exchanging a pre-shared key sets the strength of the algorithm in bits. Ensure that the DH Group is configured identically on both your device and the remote endpoint.

e. In the **IKE SA-Lifetime** field, enter the duration, in seconds, after which the Security Association for the VPN connection is renegotiated.

STEP 4 In the **Phase 2 Configuration** section, configure parameters to negotiate IPsec Security Association (SA) for the IPsec tunnel:

a. In the **Local IP** field, indicate how many endpoints will be part of the VPN policy:

- **Single**—Limits the policy to one host. Enter the IP address of the host that will be part of the VPN in the **IP Address** field.
- **Subnet**—Allows an entire subnet to connect to the VPN. Enter the network address in the **IP Address** field, and enter the subnet mask in the **Subnet Mask** field. Enter the subnet's network IP address in the **IP Address** field. Enter the subnet mask, such as 255.255.255.0, in the **Subnet Mask** field. The field automatically displays the default subnet address based on the IP address.

b. In the **IPsec SA Lifetime** field, enter the duration, in seconds, after which the IPsec Security Association for the VPN connection is renegotiated.

c. Choose the **Encryption Algorithm** to encrypt data and choose the **Authentication Algorithm** for the VPN header. Ensure that the authentication algorithm is configured identically on both your device and the remote endpoint.

d. To create a more secure IPsec VPN connection, check the **PFS Key Group Enable** check box, ensuring a new Diffie-Hellman key exchange in phase 2. Perfect Forward Secrecy (PFS) creates an additional layer of security by protecting your data with a new key, in case the DH key generated in phase 1 is compromised in transit. Ensure that both IPsec endpoints have PFS enabled.

STEP 5 Click **Save**.

Configuring IPsec VPN User Accounts

STEP 1 Choose **VPN > IPsec VPN Server > User**.

STEP 2 Click **Add Row**.

STEP 3 Enter a username and password.

We recommended 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.

STEP 4 To import usernames and passwords from a CSV file, click **Import**. The **Administration > Users** page is displayed. In the **Import Username and Password**

section, click **Browse** to locate the file, and click **Import**. See **Importing User Accounts** for more information.

STEP 5 Save your user accounts.

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.

Configuring the PPTP Server

To configure the PPTP VPN server:

STEP 1 Choose **VPN** > **PPTP Server**.

STEP 2 In the **PPTP Server Configuration** section, configure the PPTP VPN settings:

a. Check the **PPTP Server Enable** check box.

b. Enter the IP address of the PPTP server.

c. Enter the range of IP addresses for PPTP clients.

d. To encrypt the data passing through the PPTP VPN connection, check the **MPPE Encryption Enable** check box.

STEP 3 Click **Save**.

Creating and Managing PPTP Users

To create and enable PPTP users:

STEP 1 Choose VPN > PPTP Server. In the **PPTP User Account Table**, click **Add Row**.

STEP 2 Enter the username and password that will authenticate the PPTP user. Enter values that are between 4 to 32 characters long.

STEP 3 Check the **Enable** check box for the user.

STEP 4 To import usernames and passwords from a CSV file, click **Import**. The **Administration > Users** page is displayed. In the **Import Username and Password** section, click **Browse** to locate the file, and click **Import**. See **Importing User Accounts** for more information.

STEP 5 Save your user accounts.

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 Check the **Enable** check box to choose the type of traffic to allow to pass through the device.

STEP 3 Click **Save**.

7

Configuring Quality of Service (QoS)

Quality of service (QoS) assigns priority to various applications, users, or data flows, or guarantees a level of performance to a data flow. These guarantees are important when the network capacity is insufficient. For example, for real-time streaming multimedia applications such as voice-over-IP, online games, and IP-TV because they require fixed bit rate and are delay sensitive, and for networks where the capacity is a limited resource.

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. (Applies to the default VLAN only)

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

STEP 2 Enter information in the following fields:

Enable	Check to enable bandwidth management for this service.
Direction	Choose if you want to set priority for inbound or outbound traffic.
Category	Choose if you want to set bandwidth priority for a service, VLAN/SSID, Source IP (inbound traffic), or Destination IP (outbound traffic).
Service	Choose the service to prioritize.
VLAN/SSID	Choose the VLAN or SSID for which you want to set priority.
IP Address	If you select Source IP or Destination IP in the **Category** field, enter the IP address and the subnet mask of the source or destination.
Subnet Mask	
Priority	Set the priority (**low**, **medium**, or **high**) for the selected category.
Remarking	Check to enable remarking on 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.

DSCP	Enter the remarking value for packets on this network.

STEP 3 Click **Save**.

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

To delete an entry from the table, check the relevant box and click **Delete**. 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 port on your device. The supports four priority queues that allow traffic prioritization for each port.

To configure QoS settings for the ports on your device:

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

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

Trust Mode	Choose one of the following options from the drop-down menu: • **Port**—Enables port-based QoS settings. 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 3. • **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 3).

STEP 3 Click **Save**.

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

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

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

STEP 3 Click **Save**.

To restore the default port-based QoS settings, click **Restore Default** 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 whether to only list RFC values or to list all DSCP values in the **DSCP Settings Table** by clicking the relevant button.

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

This maps the DSCP value to the selected QoS queue.

STEP 4 Click **Save**.

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

8

Managing Your Device

Setting Device Properties

Assign a name and a domain name to your device to ensure that it is easily identified by other devices.

To set device properties:

STEP 1 Choose **Administration > Device Properties**.

STEP 2 In the **Hostname** field, enter a name to identify the device uniquely on your network. For example, RTR141.

STEP 3 In the **Domain Name** field, enter the domain in which your device is located. For example, abcbusiness.com. If you do not know the name of your organization's domain, contact your network administrator.

STEP 4 Save your changes.

Setting Password Complexity

You can enforce a 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 (0-64 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: an administrative user (default user name and password: cisco) and a guest user (default user name: guest).

The guest account has read-only access. You can set and change the username and password for both the administrator and guest accounts.

To configure the user accounts:

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

STEP 2 In the **Account Activation** field, check the boxes for the accounts that 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 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	Reenter the new password.

STEP 4 Click **Save**.

Importing User Accounts

You can import several users at the same time using a CSV file.

Ensure that the data in the CSV file is arranged as shown in the following tables:

TYPE	USERNAME	PASSWORD
Admin	Admin123	Admin123
Guest	Guest123	Guest123

TYPE	USERNAME	PASSWORD	ENABLE
PPTP	PPTP-user-1	12345678	enable
PPTP	PPTP-user-2	345123678	disable

TYPE	USERNAME	PASSWORD
VPNServer	vpn-user-1	12345678
VPNServer	vpn-user-2	33245678

TYPE	USERNAME	PASSWORD	ACCESS_TIME
guestnet	guestnet-user-1	12345678	1440
guestnet	guestnet-user-2	33245678	60

NOTE The names of the columns are case-sensitive. Do not change the order or the names of the columns.

To import user accounts from a CSV file:

STEP 1 In the **Import User Name & Password** field, click **Browse**.

STEP 2 Locate the file and click **Open**.

STEP 3 Click **Import**.

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

NOTE Before you can use SNMP, install SNMP software on your computer. Your device supports only SNMPv3 for SNMP management and SNMPv1/2/3 for SNMP trap messages.

To enable SNMP:

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

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

STEP 3 Select the SNMP version in the **Mode** field.

STEP 4 Enter this information:

SysContact	Enter the name of the contact person for this device. For example, your network administrator.
SysLocation	Enter the physical location of the device. For example, Rack #2, 4th Floor.
SysName	Enter a name to identify your device easily. For example, RTR 141.

STEP 5 Click **Save**.

Editing SNMPv3 Users

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

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 and 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 device 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**.
SNMP Trap Severity Level	Choose the severity level at which the device must send trap messages.

STEP 3 Click **Save**.

Using Diagnostic Tools

Your 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 if the device is reachable.

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.

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.

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 Log and E-mail Settings

Configure logs to monitor activity that indicates the health and performance of your device.

Configuring Log Settings

To configure logging:

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

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

STEP 3 Check the **Email Alert Enable** check box to configure the device to send alert emails to a specific email address for events or behavior that may impact the performance, operation, and security of the device, or for debugging purposes. Check the appropriate box to enable email alerts for the following events:

WAN up/down	Sends an email when the WAN link is down and sends another email when the link is back up again.
Site-to-site IPsec VPN Tunnel up/down	Sends an email when the site-to-site IPsec VPN tunnel is down and sends another email when the tunnel is back up again.
CPU overload	Sends an alert email if the CPU utilization is higher than the threshold and sends another alert email when the CPU utilization comes back down to normal.
System startup	Sends an email alert when the device is booting up.
New Firmware available	Sends an email alert when new firmware is available for the device.

STEP 4 Click **Add Row**.

STEP 5 Configure the following settings:

Remote Log Server	Enter the IP address of the log server that will maintain logs.
Log Severity for Local Log and Email	Choose the severity of events for which you want to maintain logs and send logs them to a specific email address. All log types that are higher in severity than the selected log type are automatically included and you cannot exclude them. For example, if you choose Error logs, Emergency, Alert, and Critical are also selected. The event severity levels are listed from the highest severity to the lowest severity: • **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**—Detailed event information. Choosing this severity of logs generates a long list of logs and is not recommended during normal router operation.
Enable	To enable these logging settings, check this box.

STEP 6 Click **Save**.

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

Configuring Log E-Mailing

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

You must first set up the severity of logs you want to capture; see **Configuring Log Settings**.

To configure the e-mailing of logs:

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

STEP 2 To receive e-mail alerts about new firmware versions, check **New Firmware E-mail Alert Enable**.

STEP 3 To enable the e-mailing of log events, check **E-mail Logs Enable**.

The minimum email log severity of logs that you want to capture appears. To change this setting, click **Configure Severity**.

STEP 4 Configure the following settings:

E-mail Server Address	Enter the address of the SMTP server. This is the mail server associated with the email account that you have setup (for example, mail.companyname.com).
E-mail Server Port	Enter the SMTP server port. If your email provider requires a special port for email, enter it here. Otherwise, use the default (25).
Return E-mail Address	Enter the return email address that the device will send messages to if logs from the router to the send-to email address are undeliverable.
Send to E-mail Address (1)	Enter an email address to which to send logs (for example, logging@companyname.com).
Send to E-mail Address (2) (Optional)	
Send to E-mail Address (3) (Optional)	

E-mail Encryption	Choose SSL or TSL as the email encryption method. Choose Disable if you do not want to use an email encryption method.
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 email authentication username (for example, logging@companyname.com).
E-mail Authentication Password	Enter the email authentication password (for example, the password used to access the email account you have set up to which to send logs).
E-mail Authentication Test	Click **Test** to test email authentication.

STEP 5 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 6 Click **Save**.

Configuring Bonjour

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

To enable Bonjour:

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

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

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

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

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

STEP 4 Click **Save**.

Configuring Date and Time Settings

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

To configure NTP and time settings:

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

STEP 2 Enter information in the following fields:

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 dimmed if you click **Manual** in the **Set Date and Time** field.
Daylight Saving Mode	If you choose **By date**, enter the specific date when daylight saving mode starts. If you choose **Recurring**, enter the month, week, day of week, and time when 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	Choose if you want the date and time on the device set manually or automatically. If you select Manual, enter the date and time in the Enter Date and Time fields.
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.

STEP 3 Click **Save**.

Backing Up and Restoring the System

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

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

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

Backing Up the Configuration Settings

To 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 have all of their previous configuration information intact. You can download the Startup Configuration to other RV130/RV130W devices for easy deployment.
Mirror configuration	Select this option if the device must 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 a backup file based on the selected configuration option, click **Download**.

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

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

Restoring the Configuration Settings

To restore a previously saved configuration file:

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

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

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

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

STEP 5 Click **Start to Upload**.

The 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 get locked out of Device Manager. To get back into Device Manager, 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

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

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 device 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 Log E-Mailing**.

STEP 5 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 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.

STEP 4 (Optional) To reset the device to default factory settings after the firmware is upgraded, check **Reset all configurations/settings to factory defaults**.

⚠ **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 flash, and the device is automatically rebooted with the new firmware.

STEP 6 Choose **Status** > **System Summary** to make sure the router installed the new firmware version.

Changing the Language

To change the language on the device:

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 (Optional) To restore the device configuration parameters to factory default values, select **Reset all configuration/settings to factory defaults**.

STEP 5 Click **Start Upgrade**.

Restarting the Device

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**.

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.
Cisco Open Source Requests	www.cisco.com/go/smallbiz_opensource_request
Cisco Partner Central (Partner Login Required)	www.cisco.com/web/partners/sell/smb

Product Documentation	
Cisco RV130/RV130W Wireless Multifunction VPN Router	www.cisco.com/en/US/products/ps9923/tsd_products_support_series_home.html