ADMINISTRATION GUIDE

Cisco RV132W ADSL2+ Wireless-N VPN Router and
Cisco RV134W VDSL2 Wireless-AC VPN Router

Contents

1

Getting Started

Thank you for choosing the Cisco RV132W ADSL2+ Wireless-N router or the Cisco RV134W VDSL2 Wireless-AC routers. This guide describes how to physically install and manage your Cisco RV132W/RV134W router. The **Getting Started** page displays the most common configurations on your device. Click the links on the Web page to go to the relevant configuration page.

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

Initial Settings

Change Default Administrator Password	Displays the **User Account** page where you can change the administrator password and set up a guest account. See **Configuring User Accounts**.
Launch Setup Wizard	Launches the **Router Setup Wizard**. Follow the on-screen instructions.
Configure WAN Settings	Opens the **Internet Setup** page to modify the WAN parameters. See **Configuring WAN Connections**.
Configure LAN Settings	Opens the **LAN Configuration** page to modify the LAN parameters. For example, the management IP address. See **Configuring LAN Connections**.
Configure Wireless Settings	Open the **Basic Settings** page to manage the wireless settings. See **Basic Wireless Settings**

Quick Access

Upgrade Router Firmware	Opens the **Firmware Upgrade** page to update the device firmware. See **Firmware Upgrade**.
Add VPN Clients (For RV134W only)	Opens the **PPTP Server** page to set up and manage the VPN tunnels. See **Configuring PPTP**.
Configure Remote Management Access	Opens the **Basic Settings** page to enable the basic features of the device. See **Basic Firewall Settings**.

Device Status

System Summary	Displays the **System Summary** page that shows the IPv4 and IPv6 configuration, wireless, and firewall status on the device. See **System Summary**.
Wireless Status	Displays the **Wireless Statistics** page that shows the state of the radio. See **Wireless Statistics**.
VPN Status (For RV134W only)	Displays the **IPsec VPN Server** page that lists the VPN managed by this device. See **PPTP Server**.

Run Setup Wizard

From the **Run Setup Wizard** page, you can follow the instructions that guide you through the process for configuring the device.

To open this page, select **Run Setup Wizard** in the navigation tree.

Follow the on-screen instructions to proceed. Refer to the information from your ISP to enter the required settings for your Internet connection.

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

Status and Statistics

Dashboard

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

To access the dashboard, select **Status and Statistics** > **Dashboard.** To modify the information displayed, click the detailed link to go to the configuration page for that section. For more information on managing the settings displayed on the Dashboard page, see:

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

From the **Refresh Rate** drop-down list, select 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.

System Summary

Select **Status and Statistics** > **System Summary** to view the Internet setup, LAN, wireless, firewall, and PPTP (for RV134W).

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

WAN Configuration

Displays the setting details for your WAN networks configured on the Networking > WAN > WAN Configuration > Internet Setup page. For more information, see **Configuring WAN Connections**

LAN Configuration

Displays the setting details for your LAN networks configured on the Networking > LAN > LAN Configuration. For more information, see **Configuring LAN Connections**

Wireless Summary

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

Firewall Setting Status

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

PPTP Server Status

Displays the available PPTP VPN connections and the connected users for each VPN type. For more information on configuring VPN server connections and user accounts, see **Configuring PPTP**.

Active TCP/IP Services

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

Wireless Statistics

Select **Status and Statistics**> **Wireless Statistics** to view the wireless statistical data for the device radio. In the **Refresh Rate** field, select 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.

PPTP Server

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

IPSec Connection Status

IPsec VPN Connection Status

STEP 1 Select **Status and Statistics > IPsec Connection Status**.

STEP 2 Select the **Refresh Rate** from the drop-down list to display the latest IPSec connections and the duration of the connection.

STEP 3 Select the **Show Simplified Statistic Data** to display the simplified statistic data.

STEP 4 Click **Save.**

View Logs

The View Logs page can only be displayed if the user enables log at **Administrator > Logging > Log Setting**. Once this is enabled to view the logs, select **Status and Statistics> View Logs**. Click **Refresh Rate,** to display latest log entries.

To filter logs or specify the severity of the logs to display, in the System Log Table, 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.
- **Information**—Messages about device information.
- **Debugging**—Detailed information about an event.

To refresh all entries in the log window, click **Refresh Logs.**

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, select a number from the drop-down list.

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

Connected Devices

The **Connected Devices** page displays information about the active client devices connected to your router. To view connected devices, select **Status and Statistics**> **Connected Devices**.

To specify the types of interfaces to display, select a value from the **Filter: Interface Type matches** drop-down list:

- **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.

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.

Port Statistics

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

To view port statistics, select **Status and Statistics > Port Statistics**.

To refresh the page at regular intervals, select 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.

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.

Mobile Network

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

To view the mobile network status, select **Status and Statistics> 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

Networking

WAN Configuration

Configuring WAN Connections

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

To configure the **Global Settings** follow these steps:

STEP 1 Select **Networking > WAN> WAN Configuration**.

STEP 2 In the **Global Settings > Connect Mode**, select one of the following:

- **Auto** (DSL->Ethernet): the device will check if the DSL link is up. If it is up, the device will use the DSL link as the WAN interface; if it is down, the device will check if the Ethernet link is up, and if it is up, it will use the Ethernet link as the WAN interface.
- **DSL**: the device will use the DSL link as the WAN interface.
- **Ethernet**: the device uses Ethernet link as the WAN interface.

STEP 3 Click **Edit (RV132W) or Add Row (RV134W)** and configure the settings for the xDSL WAN or Ethernet WAN.

Configuring xDSL WAN

When the Internet Connection Type is in Bridged Mode Only:

In the **DSL Settings** for ATM transfer mode enter the following information**:**

Transfer Mode	ATM

Multiplexing	Defines the way in which different protocols are handled within a DSL virtual circuit. You can choose between a Logical Link Control (LLC) encapsulation and Virtual Channel (VC) multiplexing.
QoS Type	Select the DSL Quality of Service (QoS): Unspecified Bit Rate (UBR), Constant Bit Rate (CBR), Variable Bit Rate - real time (VBR-rt), Variable Bit Rate - non-real time (VBR-nrt). CBR provides the best guarantee of low latency; UBR provides none, but is typically used for most broadband data services. **Pcr Rate** - When the QoS is set to CBR, VBR-rt, or VBR-nrt, enter the Peak Cell Rate (PCR) in cells per second. **Scr Rate** - When the QoS is set to VBR-nrt or VBR-rt, enter the Sustained Cell Rate (SCR) in cells per second.
Auto Detect	Check **Enable** to enable or **Disable** to disable automatic detection of the VPI and VCI values that identify your line to the ATM network.
Virtual Circuit	The **Virtual Path Identifier (VPI)** and **Virtual Channel Identifier (VCI)** are values used to identify your line to your ISP's ATM network.
SRA (Seamless Rate Adaption)	Check **Enable** or **Disable** to enable or disable the SRA, a protocol which, by decoupling the modulation and framing layer, can change the transmission data rate parameters (applied by the modulation layer).

DSL Modulation	Select the DSL modulation from the drop-down list. The default DSL modulation is **Multimode** (recommended).

In the **DSL Settings** for PTM transfer mode (RV134W) enter the following information**:**

Transfer Mode	PTM
SRA (Seamless Rate Adaption)	Check **Enable** or **Disable** to enable or disable the SRA, a protocol which, by decoupling the modulation and framing layer, can change the transmission data rate parameters (applied by the modulation layer).
DSL Modulation	Select the DSL modulation from the drop-down list. The default DSL modulation is **Multimode** (recommended).

In the **Bridged Settings** section for both the ATM and PTM (RV134W) transfer modes, enter the following information:

Ethernet LAN Ports	Select the Ethernet LAN ports. (**LAN1, LAN2, LAN3 or LAN4 -** [RV134W only]).
2.4G Wireless Ports	Select **SSID1** (default).
5G Wireless Ports (RV134W only)	Select **SSID1** (default).

In the **Other Settings** section for both the ATM and PTM (RV134W) transfer modes, enter the following information**:**

VLAN & VLAN ID	If enabled, all outbound traffic through this interface is tagged with the configured VLAN ID**.**
MTU (Maximum Transmission Unit)	MTU is an advanced configuration that allows you to determine the largest data size permitted on your connection. Select **Auto** (default) or **Manual** to configure manually.

Size	Enter the size of bytes. (Range 576 - 1500, Default 1500).

When the Internet Connection Type is RFC2684 Bridged (DHCP or Static mode)

In the **DSL Settings** for the ATM transfer mode, enter the following information:

Transfer Mode	ATM
Multiplexing	Defines the way in which different protocols are handled within a DSL virtual circuit. You can choose between a Logical Link Control (LLC) encapsulation and Virtual Channel (VC) multiplexing.
QoS Type	Select the DSL Quality of Service (QoS): Unspecified Bit Rate (UBR), Constant Bit Rate (CBR), Variable Bit Rate - real time (VBR-rt), Variable Bit Rate - non-real time (VBR-nrt). CBR provides the best guarantee of low latency; UBR provides none, but is typically used for most broadband data services. **Pcr Rate** - When the QoS is set to CBR, VBR-rt, or VBR-nrt, enter the Peak Cell Rate (PCR) in cells per second. **Scr Rate** - When the QoS is set to VBR-nrt or VBR-rt, enter the Sustained Cell Rate (SCR) in cells per second.
Auto Detect	Check **Enable** to enable or **Disable** to disable automatic detection of the VPI and VCI values that identify your line to the ATM network.

Virtual Circuit	The **Virtual Path Identifier (VPI)** and **Virtual Channel Identifier (VCI)** are values used to identify your line to your ISP's ATM network.
SRA (Seamless Rate Adaption)	Check **Enable** or **Disable** to enable or disable the SRA, a protocol which, by decoupling the modulation and framing layer, can change the transmission data rate parameters (applied by the modulation layer).
DSL Modulation	Select the DSL modulation from the drop-down list. The default DSL modulation is **Multimode** (recommended).

In the **DSL Settings** for the PTM transfer mode (RV134W), enter the following:

Transfer Mode	PTM
SRA (Seamless Rate Adaption)	Check **Enable** or **Disable** to enable or disable the SRA, a protocol which, by decoupling the modulation and framing layer, can change the transmission data rate parameters (applied by the modulation layer).
DSL Modulation	Select the DSL modulation from the drop-down list. The default DSL modulation is **Multimode** (recommended).

In the **IPoE Settings** section for both the ATM and PTM (RV134W) transfer modes, enter the following information::

Auto Get IP (DHCP)	Check **Enable** or **Disable** to enable or disable the Auto get IP (DHCP) which is a method of automatically assigning IP addresses. If disabled, manually configure the IP address.
DNS Server Source	Select **Get Dynamically from ISP** or **Use These DNS Servers** to manually configure.

Static DNS 1 & 2	Enter the IP address of the primary and or secondary Static DNS in the fields (Hint 1.2.3.4).

In the **IPv6 Settings** section for both the ATM and PTM (RV134W) transfer modes, enter the following information:

For IPv6

Mode	**IPv6**
Address Mode	Select **Dynamic** or **Static**. If you select **Dynamic**, it means that if the RA (Router Advertisement) message that the device receives, has an M Flag “0”, the device uses SLAAC (Stateless Address Auto-configuration) to get the IPv6 address; if the M Flag is “1”, the device uses DHCPv6 to get the IPv6 address. If you select **Static,** enter the following information: • IPv6 Address • IPv6 Prefix Length • Default IPv6 Gateway • IPv6 DNS1 & DNS2
Prefix Delegation	To assign a network address prefix (from ISP) to LAN, enable **Prefix Delegation**.

For 6rd

Mode	6rd
6rd Tunneling	Select **Auto** or **Manual**. If you choose **Manual**, enter the following information: • IPv6 Prefix • IPv6 Prefix Length • Border Relay • IPv4 Mask Length

In the **Other Settings** section for both the ATM and PTM (RV134W) transfer modes, enter the following information**:**

NAT (Network Address Translation)	If enabled, all outbound traffic through this interface is NAT'ed. If disable, all outbound traffic through this interface is routed.
VLAN & VLAN ID	If enabled, all outbound traffic through this interface is tagged with the configured VLAN ID**.**
802.1p Priority (For ATM transfer mode only)	Enter a range from 0 to 7. All outbound traffic of this interface will be tagged with the configured 802.1p priority. If it conflicts with the QoS setting, the QoS setting will take precedence.
MTU (Maximum Transmission Unit)	MTU is an advanced configuration that allows you to determine the largest data size permitted on your connection. Select **Auto** (default) or **Manual** to configure manually.
Size	Enter the size of bytes. (Range 576 - 1500, Default 1500).
MAC Address Clone	At times, you may need to set the MAC address of the device WAN port to be identical to your PC or some other MAC address. This is called MAC address cloning. For example, some ISPs register your computer's 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's MAC address. To configure a MAC address clone select **Enable**.

MAC Address	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.

When the Internet Connection Type is RFC2684 Routed (IPoA)

In the **DSL Settings** section, enter the following information:

Transfer Mode	ATM
Multiplexing	Defines the way in which different protocols are handled within a DSL virtual circuit. You can choose between a Logical Link Control (LLC) encapsulation and Virtual Channel (VC) multiplexing.
QoS Type	Select the DSL Quality of Service (QoS): Unspecified Bit Rate (UBR), Constant Bit Rate (CBR), Variable Bit Rate - real time (VBR-rt), Variable Bit Rate - non-real time (VBR-nrt). CBR provides the best guarantee of low latency; UBR provides none, but is typically used for most broadband data services. **Pcr Rate** - When the QoS is set to CBR, VBR-rt, or VBR-nrt, enter the Peak Cell Rate (PCR) in cells per second. **Scr Rate** - When the QoS is set to VBR-nrt or VBR-rt, enter the Sustained Cell Rate (SCR) in cells per second.
Auto Detect	Check **Enable** to enable or **Disable** to disable automatic detection of the VPI and VCI values that identify your line to the ATM network.

Virtual Circuit	The **Virtual Path Identifier (VPI)** and **Virtual Channel Identifier (VCI)** are values used to identify your line to your ISP's ATM network.
SRA (Seamless Rate Adaption)	Check **Enable** or **Disable** to enable or disable the SRA, a protocol which, by decoupling the modulation and framing layer, can change the transmission data rate parameters (applied by the modulation layer).
DSL Modulation	Select the DSL modulation from the drop-down list. The default DSL modulation is **Multimode** (recommended).

In the **IPoA Settings** section, enter the following information**:**

Internet IP Address	Enter the IP address (Hint 192.168.100.100).
Subnet Mask	Enter the subnet mask (Hint 255.255.255.0).
Default Gateway	Enter the default gateway (Hint 192.168.100.1).
Static DNS 1 & 2	Enter the IP address of the primary and or secondary Static DNS in the fields (Hint 1.2.3.4).

In the **Other Settings** section, enter the following information**:**

NAT (Network Address Translation)	If enabled, all outbound traffic through this interface is NAT'ed. If disable, all outbound traffic through this interface is routed.
MTU (Maximum Transmission Unit)	MTU is an advanced configuration that allows you to determine the largest data size permitted on your connection. Select **Auto** (default) or **Manual** to configure manually.
Size	Enter the size of bytes. (Range 576 - 1500, Default 1500).

When the Internet Connection Type is PPPoE:

In the **DSL Settings** for the ATM transfer mode, enter the following information:

Transfer Mode	ATM
Multiplexing	Defines the way in which different protocols are handled within a DSL virtual circuit. You can choose between a Logical Link Control (LLC) encapsulation and Virtual Channel (VC) multiplexing.
QoS Type	Select the DSL Quality of Service (QoS): Unspecified Bit Rate (UBR), Constant Bit Rate (CBR), Variable Bit Rate - real time (VBR-rt), Variable Bit Rate - non-real time (VBR-nrt). CBR provides the best guarantee of low latency; UBR provides none, but is typically used for most broadband data services. **Pcr Rate** - When the QoS is set to CBR, VBR-rt, or VBR-nrt, enter the Peak Cell Rate (PCR) in cells per second. **Scr Rate** - When the QoS is set to VBR-nrt or VBR-rt, enter the Sustained Cell Rate (SCR) in cells per second.
Auto Detect	Check **Enable** to enable or **Disable** to disable automatic detection of the VPI and VCI values that identify your line to the ATM network.
Virtual Circuit	The **Virtual Path Identifier (VPI)** and **Virtual Channel Identifier (VCI)** are values used to identify your line to your ISP's ATM network.

SRA (Seamless Rate Adaption)	Check **Enable** or **Disable** to enable or disable the SRA, a protocol which, by decoupling the modulation and framing layer, can change the transmission data rate parameters (applied by the modulation layer).
DSL Modulation	Select the DSL modulation from the drop-down list. The default DSL modulation is **Multimode** (recommended).

In the **DSL Settings** for the PTM transfer mode(RV134W), enter the following information:

Transfer Mode	PTM
SRA (Seamless Rate Adaption)	Check **Enable** or **Disable** to enable or disable the SRA, a protocol which, by decoupling the modulation and framing layer, can change the transmission data rate parameters (applied by the modulation layer).
DSL Modulation	Select the DSL modulation from the drop-down list. The default DSL modulation is **Multimode** (recommended).

In the **PPPoE Settings** section for both the ATM and PTM (RV134W) transfer modes, enter the following information:

Username	Enter the username.
Password	Enter the password.
DNS Server Source	Select **Get Dynamically from ISP** or **Use These DNS Servers** to manually configure.
Static DNS 1 & 2	Enter the IP address of the primary and or secondary Static DNS in the fields (Hint 1.2.3.4).

Connect on Demand Max Idle Time	Select this option if your ISP charges when you are connected to the Internet. If you select this option, the Internet connection is on - only when traffic is present. If the connection is idle - no traffic is flowing - the connection is closed. If you 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	Select the authentication type from the drop-down list. **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. **CHAP** - Challenge Handshake Authentication Protocol. **MS-CHAP** - Microsoft version of the Challenge-Handshake Authentication Protocol. **MS-CHAP2** - Microsoft version of the Challenge-Handshake Authentication Protocol version 2.
Service Name	Enter the service name.

In the **IPv6 Settings** section for both the ATM and PTM (RV134W) transfer modes, enter the following information**:**

For IPv6

Mode	**IPv6**

Address Mode	Select **Dynamic** or **Static**. If you select **Dynamic**, it means that if the RA (Router Advertisement) message that the device receives, has an M Flag “0”, the device uses SLAAC (Stateless Address Auto-configuration) to get the IPv6 address; if the M Flag is “1”, the device uses DHCPv6 to get the IPv6 address. If you select **Static,** enter the following information: • IPv6 Address • IPv6 Prefix Length • Default IPv6 Gateway • IPv6 DNS1 & DNS2 The IPv6 connection is PPPoE as well. The IPv4 and IPv6 connection share the same PPPoE setting.
Prefix Delegation	To assign a network address prefix (from ISP) to LAN, enable **Prefix Delegation**.

For 6rd

Mode	**6rd**
6rd Tunneling	Select **Auto** or **Manual**. If you choose **Manual**, enter the following information: • IPv6 Prefix • IPv6 Prefix Length • Border Relay • IPv4 Mask Length

In the **Other Settings** section for the ATM and PTM (RV134W) transfer modes, enter the following**:**

NAT (Network Address Translation)	If enabled, all outbound traffic through this interface is NAT’ed. If disable, all outbound traffic through this interface is routed.

VLAN & VLAN ID	If enabled, all outbound traffic through this interface is tagged with the configured VLAN ID**.**
Reset Timer	For PPPoE only: Reset the PPPoE connection at a given time of day and day of the week. Choose one of the following options from the **Frequency** drop-down list and specify the corresponding settings: **Never**: Choose this option to disable this feature. **Daily**: Choose this option to reset the PPPoE connection at a given time of day. Specify the time of day in the Time field. **Weekly**: Choose this option to reset the PPPoE connection at a given day of the week. Then specify the day of the week and time of day
MTU (Maximum Transmission Unit)	MTU is an advanced configuration that allows you to determine the largest data size permitted on your connection. Select **Auto** (default) or **Manual** to configure manually.
Size	Enter the size of bytes. (Range 576 - 1492, Default 1492).
MAC Address Clone	Sometimes, you may need to set the MAC address of the device WAN port to be identical to 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 select **Enable.**

MAC Address	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.

When the Internet Connection Type is PPPoA:

In the **DSL Settings** section, enter the following information:

Transfer Mode	ATM
Multiplexing	Defines the way in which different protocols are handled within a DSL virtual circuit. You can choose between a Logical Link Control (LLC) encapsulation and Virtual Channel (VC) multiplexing.
QoS Type	Select the DSL Quality of Service (QoS): Unspecified Bit Rate (UBR), Constant Bit Rate (CBR), Variable Bit Rate - real time (VBR-rt), Variable Bit Rate - non-real time (VBR-nrt). CBR provides the best guarantee of low latency; UBR provides none, but is typically used for most broadband data services. **Pcr Rate** - When the QoS is set to CBR, VBR-rt, or VBR-nrt, enter the Peak Cell Rate (PCR) in cells per second. **Scr Rate** - When the QoS is set to VBR-nrt or VBR-rt, enter the Sustained Cell Rate (SCR) in cells per second.
Auto Detect	Check **Enable** to enable or **Disable** to disable automatic detection of the VPI and VCI values that identify your line to the ATM network.
Virtual Circuit	The **Virtual Path Identifier (VPI)** and **Virtual Channel Identifier (VCI)** are values used to identify your line to your ISP's ATM network.
SRA (Seamless Rate Adaption)	Check **Enable** or **Disable** to enable or disable the SRA, a protocol which, by decoupling the modulation and framing layer, can change the transmission data rate parameters (applied by the modulation layer).

DSL Modulation	Select the DSL modulation from the drop-down list. The default DSL modulation is **Multimode** (recommended).

In the **PPPoA Settings** section, enter the following information:

Username	Enter the username.
Password	Enter the password.
DNS Server Source	Select **Get Dynamically from ISP** or **Use These DNS Servers** to manually configure.
Static DNS 1 & 2	Enter the IP address of the primary and or secondary Static DNS in the fields (Hint 1.2.3.4).
Connect on Demand Max Idle Time	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 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	Select the authentication type from the drop-down list. **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. **CHAP** - Challenge Handshake Authentication Protocol. **MS-CHAP** - Microsoft version of the Challenge-Handshake Authentication Protocol. **MS-CHAP2** - Microsoft version of the Challenge-Handshake Authentication Protocol version 2.

In the **IPv6 Settings** section, enter the following information:

For IPv6

Mode	IPv6
Address Mode	Select **Dynamic** or **Static**. If you select **Dynamic**, it means that if the RA (Router Advertisement) message that the device receives, has an M Flag “0”, the device uses SLAAC (Stateless Address Auto-configuration) to get the IPv6 address; if the M Flag is “1”, the device uses DHCPv6 to get the IPv6 address. If you select **Static,** enter the following information: • IPv6 Address • IPv6 Prefix Length • Default IPv6 Gateway • IPv6 DNS1 & DNS2 The IPv6 connection is PPPoA as well. The IPv4 and IPv6 connection share the same PPPoA setting.

Prefix Delegation	To assign a network address prefix (from ISP) to LAN, enable **Prefix Delegation**.

For 6rd

Mode	6rd
6rd Tunneling	Select **Auto** or **Manual**. If you choose **Manual**, enter the following information: • IPv6 Prefix • IPv6 Prefix Length • Border Relay • IPv4 Mask Length

In the **Other Settings** section, enter the following information:

NAT (Network Address Translation)	If enabled, all outbound traffic through this interface is NAT'ed. If disable, all outbound traffic through this interface is routed.
MTU (Maximum Transmission Unit)	MTU is an advanced configuration that allows you to determine the largest data size permitted on your connection. Select **Auto** (default) or **Manual** to configure manually.
Size	Enter the size of bytes. (Range 576 - 1492, Default 1492).

MAC Address Clone	Sometimes, you may need to set the MAC address of the device WAN port to be identical to 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 select **Enable.**
MAC Address	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.

Configuring Ethernet WAN

When the Internet Type is DHCP:

In the **DCHP Settings** section, enter the following information:

DNS Server Source	Select **Get Dynamically from ISP** or **Use These DNS Servers** to manually configure.
Static DNS1 & 2	Enter the IP address of the primary and or secondary Static DNS in the fields (Hint 1.2.3.4).

In the **IPv6 Settings** section, enter the following information:

For IPv6

Mode	IPv6

Address Mode	Select **Dynamic** or **Static**. If you select **Dynamic**, it means that if the RA (Router Advertisement) message that the device receives, has an M Flag “0”, the device uses SLAAC (Stateless Address Auto-configuration) to get the IPv6 address; if the M Flag is “1”, the device uses DHCPv6 to get the IPv6 address. If you select **Static,** enter the following information: • IPv6 Address • IPv6 Prefix Length • Default IPv6 Gateway • IPv6 DNS1 & DNS2
Prefix Delegation	To assign a network address prefix (from ISP) to LAN, enable **Prefix Delegation**.

For 6rd

Mode	6rd
6rd Tunneling	Select **Auto** or **Manual**. If you choose **Manual**, enter the following information: • IPv6 Prefix • IPv6 Prefix Length • Border Relay • IPv4 Mask Length

In the **Other Settings** section, enter the following information**:**

NAT (Network Address Translation)	If enabled, all outbound traffic through this interface is NAT’ed. If disable, all outbound traffic through this interface is routed.
MTU (Maximum Transmission Unit)	MTU is an advanced configuration that allows you to determine the largest data size permitted on your connection. Select **Auto** (default) or **Manual** to configure manually.

Size	Enter the size of bytes. (Range 576 - 1500, Default 1500).
MAC Address Clone	Sometimes, you may need to set the MAC address of the device WAN port to be identical to 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 select **Enable.**
MAC Address	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.

When Internet Connection Type is Static IP:

In the **Static IP** Settings section, enter the following 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.
Static DNS1 & 2	Enter the IP address of the primary and or secondary Static DNS in the fields (Hint 1.2.3.4).

In the **IPv6 Settings** section, enter the following information:

For IPv6

Mode	IPv6

Address Mode	Select **Dynamic** or **Static**. If you select **Dynamic**, it means that if the RA (Router Advertisement) message that the device receives, has an M Flag “0”, the device uses SLAAC (Stateless Address Auto-configuration) to get the IPv6 address; if the M Flag is “1”, the device uses DHCPv6 to get the IPv6 address. If you select **Static,** enter the following information: • IPv6 Address • IPv6 Prefix Length • Default IPv6 Gateway • IPv6 DNS1 & DNS2
Prefix Delegation	To assign a network address prefix (from ISP) to LAN, enable **Prefix Delegation**.

For 6rd

Mode	6rd
6rd Tunneling	Select **Auto** or **Manual**. If you choose **Manual**, enter the following information: • IPv6 Prefix • IPv6 Prefix Length • Border Relay • IPv4 Mask Length

In the **Other Settings** section, enter the following information:

NAT (Network Address Translation)	If enabled, all outbound traffic through this interface is NAT’ed. If disable, all outbound traffic through this interface is routed.
VLAN & VLAN ID	If enabled, all outbound traffic through this interface is tagged with the configured VLAN ID.

802.1p Priority	Enter a range from 0 to 7. All outbound traffic of this interface will be tagged with the configured 802.1p priority. If it conflicts with the QoS setting, the QoS setting will take precedence.
MTU (Maximum Transmission Unit)	MTU is an advanced configuration that allows you to determine the largest data size permitted on your connection. Select **Auto** (default) or **Manual** to configure manually.
Size	Enter the size of bytes. (Range 576 - 1500, Default 1500).
MAC Address Clone	Sometimes, you may need to set the MAC address of the device WAN port to be identical to 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 select **Enable**.
MAC Address	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.

When the Internet Connection Type is PPPoE:

In the **PPPoE Settings** section, enter the following information**:**

Username	Enter the username.
Password	Enter the password.

DNS Server Source	Select **Get Dynamically from ISP** or **Use These DNS Servers** to manually configure.
Static DNS 1 & 2	Enter the IP address of the primary and or secondary Static DNS in the fields (Hint 1.2.3.4).
Connect on Demand Max Idle Time	Select this option if your ISP charges when you are connected to the Internet. If you select this option, the Internet connection is on - only when traffic is present. If the connection is idle - no traffic is flowing - the connection is closed. If you 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	Select the authentication type from the drop-down list. **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. **CHAP** - Challenge Handshake Authentication Protocol. **MS-CHAP** - Microsoft version of the Challenge-Handshake Authentication Protocol. **MS-CHAP2** - Microsoft version of the Challenge-Handshake Authentication Protocol version 2.
Service Name	Enter the service name.

In the **IPv6 Settings** section, enter the following information:

For IPv6

Mode	IPv6

Address Mode	Select **Dynamic** or **Static**. If you select **Dynamic**, it means that if the RA (Router Advertisement) message that the device receives, has an M Flag “0”, the device uses SLAAC (Stateless Address Auto-configuration) to get the IPv6 address; if the M Flag is “1”, the device uses DHCPv6 to get the IPv6 address. If you select **Static,** enter the following information: • IPv6 Address • IPv6 Prefix Length • Default IPv6 Gateway • IPv6 DNS1 & DNS2 The IPv6 connection is PPPoE as well. The IPv4 and IPv6 connection share the same PPPoE setting.
Prefix Delegation	To assign a network address prefix (from ISP) to LAN, enable **Prefix Delegation**.

For 6rd

Mode	6rd
6rd Tunneling	Select **Auto** or **Manual**. If you choose **Manual**, enter the following information: • IPv6 Prefix • IPv6 Prefix Length • Border Relay • IPv4 Mask Length

In the **Other Settings** section, enter the following information:

NAT (Network Address Translation)	If enabled, all outbound traffic through this interface is NAT’ed. If disable, all outbound traffic through this interface is routed.

VLAN & VLAN ID	If enabled, all outbound traffic through this interface is tagged with the configured VLAN ID**.**
802.1p Priority	Enter a range from 0 to 7. All outbound traffic of this interface will be tagged with the configured 802.1p priority. If it conflicts with the QoS setting, the QoS setting will take precedence.
Reset Timer	For PPPoE only: Reset the PPPoE connection at a given time of day and day of the week. Choose one of the following options from the **Frequency** drop-down list and specify the corresponding settings: **Never**: Choose this option to disable this feature. **Daily**: Choose this option to reset the PPPoE connection at a given time of day. Specify the time of day in the Time field. **Weekly**: Choose this option to reset the PPPoE connection at a given day of the week. Then specify the day of the week and time of day.
MTU (Maximum Transmission Unit)	MTU is an advanced configuration that allows you to determine the largest data size permitted on your connection. Select **Auto** (default) or **Manual** to configure manually.
Size	Enter the size of bytes. (Range 576 - 1492, Default 1492).
MAC Address Clone	Sometimes, you may need to set the MAC address of the device WAN port to be identical to 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 select **Enable.**

MAC Address	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.

When the Internet Connection Type is L2TP (RV134W):

In the **L2TP Settings** section, enter the following information:

Auto Get IP (DHCP)	Check **Enable** or **Disable** to enable or disable the Auto get IP (DHCP) which is a method of automatically assigning IP addresses. If disabled, manually configure the IP address.
L2TP Server	Enter IP address (Hint 192.168.1.10).
Username	Enter the username.
Password	Enter the password.
DNS Server Source	Select **Get Dynamically from ISP** or **Use These DNS Servers** to manually configure.
Static DNS 1 & 2	Enter the IP address of the primary and or secondary Static DNS in the fields (Hint 1.2.3.4).
Connect on Demand Max Idle Time	Select this option if your ISP charges when 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.

In the **IPv6 Settings** section, enter the following information:

For IPv6

Mode	IPv6
Address Mode	Select **Dynamic** or **Static**. If you select **Dynamic**, it means that if the RA (Router Advertisement) message that the device receives, has an M Flag “0”, the device uses SLAAC (Stateless Address Auto-configuration) to get the IPv6 address; if the M Flag is “1”, the device uses DHCPv6 to get the IPv6 address. If you select **Static,** enter the following information: • IPv6 Address • IPv6 Prefix Length • Default IPv6 Gateway • IPv6 DNS1 & DNS2
Prefix Delegation	To assign a network address prefix (from ISP) to LAN, enable **Prefix Delegation**.

For 6rd

Mode	6rd
6rd Tunneling	Select **Auto** or **Manual**. If you choose **Manual**, enter the following information: • IPv6 Prefix • IPv6 Prefix Length • Border Relay • IPv4 Mask Length

In the **Other Settings** section, enter the following:

NAT (Network Address Translation)	If enabled, all outbound traffic through this interface is NAT’ed. If disable, all outbound traffic through this interface is routed.

VLAN & VLAN ID	If enabled, all outbound traffic through this interface is tagged with the configured VLAN ID**.**
802.1p Priority	Enter a range from 0 to 7. All outbound traffic of this interface will be tagged with the configured 802.1p priority. If it conflicts with the QoS setting, the QoS setting will take precedence.
MTU (Maximum Transmission Unit)	MTU is an advanced configuration that allows you to determine the largest data size permitted on your connection. Select **Auto** (default) or **Manual** to configure manually.
Size	Enter the size of bytes. (Range 576 - 1460, Default 1460).
MAC Address Clone	Sometimes, you may need to set the MAC address of the device WAN port to be identical to 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 select **Enable.**
MAC Address	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.

When the Internet Connection Type is PPTP:

In the **PPTP Setting** section, enter the following information:

Auto Get IP (DHCP)	Check **Enable** or **Disable** to enable or disable the Auto get IP (DHCP) which is a method of automatically assigning IP addresses. If disabled, manually configure the IP address.
PPTP Server Type	Select **IP Address** or **FQDN.**
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.
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**.
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.
MPPE Encryption	Microsoft Point-to-Point Encryption (MPPE) encrypts data in Point-to-Point Protocol (PPP)-based dial-up connections or Point-to-Point Tunneling Protocol (PPTP) virtual private network (VPN) connections. Check **Enable** to activate MPPE encryption.

In the **IPv6 Settings** section, enter the following information

For IPv6

Mode	IPv6

Address Mode	Select **Dynamic** or **Static**. If you select **Dynamic**, it means that if the RA (Router Advertisement) message that the device receives, has an M Flag “0”, the device uses SLAAC (Stateless Address Auto-configuration) to get the IPv6 address; if the M Flag is “1”, the device uses DHCPv6 to get the IPv6 address. If you select **Static,** enter the following information: • IPv6 Address • IPv6 Prefix Length • Default IPv6 Gateway • IPv6 DNS1 & DNS2
Prefix Delegation	To assign a network address prefix (from ISP) to LAN, enable **Prefix Delegation**.

For 6rd

Mode	6rd
6rd Tunneling	Select **Auto** or **Manual**. If you choose **Manual**, enter the following information: • IPv6 Prefix • IPv6 Prefix Length • Border Relay • IPv4 Mask Length

In the **Other Settings** section, enter the following:

NAT (Network Address Translation)	If enabled, all outbound traffic through this interface is NAT’ed. If disable, all outbound traffic through this interface is routed.
VLAN & VLAN ID	If enabled, all outbound traffic through this interface is tagged with the configured VLAN ID**.**

802.1p Priority	Enter a range from 0 to 7. All outbound traffic of this interface will be tagged with the configured 802.1p priority. If it conflicts with the QoS setting, the QoS setting will take precedence.
MTU (Maximum Transmission Unit)	MTU is an advanced configuration that allows you to determine the largest data size permitted on your connection. Select **Auto** (default) or **Manual** to configure manually.
Size	Enter the size of bytes. (Range 576 - 1460, Default 1460).
MAC Address Clone	Sometimes, you may need to set the MAC address of the device WAN port to be identical to 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 select **Enable**.
MAC Address	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.

Configuring a Mobile Network

Choose **Networking > WAN > Mobile Network** 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	Username and password provided by your mobile network service provider.
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**.
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.

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 DSL or 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 DSL/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.

LAN Configuration

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 configure manually 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.

Configuring LAN Connections

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 Select **Networking** > **LAN** > **LAN Configuration**.

STEP 2 In the Network section, enter this information

Host Name	Host name
Domain Name	Domain name

STEP 3 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 used by another device.
Subnet mask	Subnet mask for the local IP address. The default subnet mask is 255.255.255.0.

STEP 4 In the Server Settings (DHCP), 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:

Default Gateway IP Address	The default gateway IP address is the gateway IP address assigned to the DHCP client.
Start IP Address	The first address in the IP address pool. Any DHCP client joining the LAN is assigned an IP address in this range.

End IP Address	The last address in the IP address pool. Any DHCP client joining the LAN is assigned an IP address in this range.
Client Lease time	Duration (in minutes) that IP addresses are leased to clients.
DNS Server	Select DNS server from the drop-down list.
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.
DHCP Option 66/150 & 67	Check Enable to enable DCHP option 66/150 & 67.
TFTP Server Host Name	Option 66, name of the TFTP server host.
TFTP Server IP	Option 150, IP address if the TFTP server.
Configuration Filename	Option 67, name of the configuration file.

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

STEP 5 Click **Save**.

Configuring VLAN Membership

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 five other VLANs on the device.

To create a VLAN:

STEP 1 Select **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 2 to 4094. VLAN ID 1 is reserved for the default VLAN, and is used for untagged frames received on the interface.
Description	A description that identifies the VLAN.
Inter-VLAN Routing	Inter-VLAN routing is the capability to route traffic between vlans. Check **Disable** to disable.
Port 1 **Port 2** **Port 3** **Port 4 (Available only on the RV134W)**	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. Select 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 Select **Networking > LAN > Static DHCP**.

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

STEP 3 Click **Add Row**.

STEP 4 Enter the following information:

Description	Description of the client
IP Address	The IP address you want assigned to the client device. 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 MAC address format is XX:XX:XX:XX:XX:XX where X is a number from 0 to 9 or a letter between A and F.

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, select **Networking > LAN > DHCP Leased Client Tables.**

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 recommend that you place hosts that must be exposed to the WAN (such as web or e-mail servers) in the DMZ network. You can configure the 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 Select **Networking** > **LAN** > **DMZ Host**.

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

STEP 3 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 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 Select **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	Select from the drop-down menu one of the following port speeds: • **Auto Negotiation**—The device and the connected device select a common speed. • **10Mbps Half**—10 Mbps in both directions, but only one direction at a time. • **10Mbps Full**—10 Mbps in both directions simultaneously. • **100Mbps Half**—100 Mbps in both directions, but only one direction at a time. • **100Mbps Full**—100 Mbps in both directions simultaneously.
Flow Control	Check to enable flow control for this port. Flow control is the process of managing the rate of data transmission between two nodes to prevent a fast sender from outrunning a slow receiver. It provides a mechanism for the receiver to control the transmission speed, so that the receiving node is not overwhelmed with data from the transmitting node.
EEE	Check this box to enable Energy-Efficient Ethernet that reduces the consumption of power during periods of low activity. This function is only available on RV134W.

STEP 3 Click **Save**.

Configuring Routing

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

Configuring Basic Routing

To configure basic routing mode:

STEP 1 Select **Networking > Routing > Basic Routing**.

STEP 2 In the **Static Routing section**, configure the following information:

Route Entries	Select the number of entries from the drop-down list.
Enter Route Name	Name of the route.
Destination LAN IP	IP address of the destination LAN.
Subnet Mask	Subnet mask address.
Gateway	Gateway address.
Interface	Select interface by checking LAN & Wireless or Internet (WAN).

STEP 3 Click **Save**.

Configuring Dynamic Routing Information Protocol (RIP)

Routing Information Protocol 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 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 destination.

NOTE The RIP is disabled by default on the device.

To configure dynamic RIP:

STEP 1 Select **Networking** > **Routing**> RIP.

STEP 2 In the RIP Basic Settings, configure the following settings:

RIP Status	Check On to enable and Off to disable RIP.
RIP Version	Select the RIP Version (**RIPv1** or **RIPv2** or Default [receive RIPv1, send 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.

STEP 3 In the RIP Members area, check **Enable RIP** to enable RIP on all available interfaces (i.e. VLAN1, DSL_ATM, ETH_WAN, DSL_PTM).

STEP 4 Click **Edit** to specify the following RIP authentication settings for an interface:

STEP 5 In the RIP Authentication Settings, in Authentication, specify the authentication method for the port.

- **None:** Choose this option to invalidate the authentication.
- **Simple Password Authentication**: Choose this option to validate the simple password authentication. Enter the password in the field.
- **MD5 Authentication:** Choose this option to validate the MD5 authentication.
- **MD5 Key ID**: Enter a numerical range from 1 to 255; default is 1.
- **MD5 Auth Key**: Enter the MD5 authentication key (Length 1 to 64 characters).

STEP 6 Passive Interface determines how the router receives the RIP packets. Check **Passive Interface** to enable on the port.

STEP 7 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, select **Networking** > **Routing Table** and select 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 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 Select **Networking** > **Dynamic DNS**.

STEP 2 You can disable Dynamic DNS or enable a **DDNS Service** on the device from the drop-down list.

STEP 3 If you select to enable one of the DDNS services (DynDNS.com, noip.com) configure the following 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.
Verify Password	Verify password of the DDNS.
Timeout	Set the number (in hours) that you wish the device to timeout.

Host Name	The name of the host account.
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 4 Click **Test Configuration,** to test the DDNS configuration.

STEP 5 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 Select **Networking** > **IP Mode**.

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

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

STEP 3 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 LAN properties for an IPv6 network depends on the type of Internet connection that you have.

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 the 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 the following mode:

- 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 Select **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 server settings (DHCPv6):

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.
DNS Server	Select DNS Server name from the drop-down list.
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 minutes) for which IPv6 addresses are leased to endpoints on the LAN.

STEP 5 In the **IPv6 Address Pool Table**, click **Add Row and enter the following 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 6 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 Select **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 **DSL-WAN**.
Metric	Priority of the route. Select 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 Select **Networking** > **IPv6** > **Routing (RIPng)**.

STEP 2 In the RIPng field, check **Enable**.

STEP 3 In the RIP Members table, select the Index and Interface from the list and check **Enable** in the corresponding RIPng and Passive Interface columns

STEP 4 Click **Save**.

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 Select **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	Select **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 exist on the router. The default is 1800 seconds.

STEP 3 Click **Save**.

Configuring Advertisement Prefixes

To configure the RADVD available prefixes:

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

STEP 2 Click **Add Row**.

STEP 3 Enter the following information:

IPv6 Prefix	The IPv6 prefix specifies the IPv6 network address.

IPv6 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

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 a name, 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. You can prevent or permit the specified devices to access the wireless network. 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.

- 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.

Basic Wireless Settings

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. These tables describe the default settings of these networks.

SSID Name for RV132W	ciscosb1	ciscosb2	ciscosb3	ciscosb4
Enabled	Yes	No	No	No
SSID Broadcast	Enabled	Enabled	Enabled	Enabled
Security Mode	WPA2-Personal	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
WPS	Enabled	Disabled	Disabled	Disabled

SSID Name for RV134W	ciscosb1_2.4G or ciscosb1_5G	ciscosb2_2.4G or ciscosb2_5G	ciscosb3_2.4G or ciscosb3_5G	ciscosb4_2.4G or ciscosb4_5G
Enabled	Yes	No	No	No
SSID Broadcast	Enabled	Disabled	Disabled	Disabled
Security Mode	WPA2-Personal	Disabled	Disabled	Disabled
MAC Filter	Disabled	Disabled	Disabled	Disabled

SSID Name for RV134W	ciscosb1_2.4G or ciscosb1_5G	ciscosb2_2.4G or ciscosb2_5G	ciscosb3_2.4G or ciscosb3_5G	ciscosb4_2.4G or ciscosb4_5G
VLAN	1	1	1	1
Wireless Isolation with SSID	Disabled	Disabled	Disabled	Disabled
WMM	Enabled	Enabled	Enabled	Enabled
WPS	Enabled for 2.4G but Disabled by default for 5G	Disabled	Disabled	Disabled

Configuring Wireless Settings

Select **Wireless > Basic Settings** to configure basic wireless settings.

To configure basic wireless settings

Select **Wireless > Basic Settings**.

STEP 1 In the Radio field, check **Enable** to turn on the wireless radio. By default, there is only one wireless network enabled, **ciscosb1**.

STEP 2 In the **Wireless Network Mode** field, select one of these options from the drop-down list: (For the RV132W and RV134W 2.4G option.)

B/G/N-Mixed	If you have Wireless-N, Wireless-B, and Wireless-G devices in your network. This is the default setting for the RV132W & RV134 2.4G (recommended).
B Only	Select this option if you have only Wireless-B devices in your network.
G Only	Select this option if you have only Wireless-G devices in your network.
N Only	Select this option if you have only Wireless-N devices in your network.
B/G-Mixed	Select this option if you have Wireless-B and Wireless-G devices in your network.

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

STEP 3 If you chose the default setting **B/G/N-Mixed,** the wireless bandwidth in the Wireless Band Selection should be set at **20MHz (default).** If you choose **N-Only,** or **G/N Mixed**, in the Wireless Band Selection field, select the wireless bandwidth on your network **(20MHz or 20/40MHz)**.

STEP 4 Optional and applicable to configure the **RV134W 5G Wireless Channel Width** settings.

A-Only	Select this option if you have only Wireless-A devices in your network.
N/AC-Mixed	Select this option if you have Wireless-N and Wireless-AC devices in your network.
A/N/AC-Mixed	Select this option if you have Wireless-A, Wireless-N and Wireless-AC devices in your network. This is the default setting for the RV134 5G (recommended).

STEP 5 In the **Wireless Channel Width** field, select **80MHZ** (Default for RV134W).

STEP 6 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 7 (Optional) In the **Wireless Table**, configure the settings of the four wireless networks.

STEP 8 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	Select the VLAN associated with the network.
Wireless Isolation with SSID	Check this box to enable wireless isolation within the SSID.
WMM (Wi-Fi Multimedia)	Check this box to enable WMM.
WPS	Check this box to map the device WPS button on the front panel to this network.

STEP 4 Click **Save**.

Configuring the Security Mode

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

Configuring WEP

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

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

To configure the WEP security mode:

STEP 1 Select **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, select the SSID for which to configure the security settings.

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

STEP 5 In the **Authentication Type** field, select 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, select the encryption type:

- **10/64-bit (10 hex digits)**—Provides a 40-bit key.
- **26/128-bit (26 hex digits)**—Provides a 104-bit key, which offers stronger encryption, making the key more difficult to 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 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, select 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 WPA2-Personal and WPA2-Personal Mixed.

- The WPA2 Personal, and WPA2 Personal Mixed, WPA2 Enterprise and WPA2 Enterprise Mixed security modes offer strong security to replace WEP.
- **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 WPA2 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**, select the SSID for which to configure the security settings.

STEP 4 From the **Security Mode** menu, select one of the two WPA2 Personal options.

STEP 5 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 6 To show the security key as you are entering it, check the **Unmask Password** box.

STEP 7 In the **Key Renewal** field, enter the duration of time (600–7200 seconds) between key renewals. The default value is 3600.

STEP 8 Click **Save** to save your settings. Click **Back** to go back to the **Basic Settings** page.

Configuring WPA2-Enterprise and WPA2-Enterprise Mixed

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

- **WPA2-Enterprise**—Allows you to use WPA2 to connect using the RADIUS server authentication.
- **WPA2-Enterprise Mixed**—Allows WPA2 client to connect using the RADIUS server authentication.

To configure the WPA2 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, select the SSID for which to configure the security settings.

STEP 4 From the **Security Mode** menu, select one of the two WPA2 Enterprise options.

STEP 5 In the **RADIUS Server** field, enter the IP address of the RADIUS server.

STEP 6 In the **RADIUS Port** field, enter the port used to access the RADIUS server.

STEP 7 In the **Shared Key** field, enter an alphanumeric phrase.

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

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

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

Configuring 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, select 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 Select **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 (disabled).
WMM No Acknowledgment	Enabling WMM No Acknowledgment 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.**

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 Select **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 — 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.

  Enable AP with Enrollee PIN — Check to make “PIN Lifetime” editable manually.

Preshared Key — Choose “Add Client to existing network (Use Existing PSK)” or “Reconfigure network (Generate New PSK)”.

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

5

Firewall

You can secure your network by creating and applying the rules that the device uses to selectively block and allow inbound and outbound Internet traffic. You can 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 and custom services that you define.
- Direction of traffic by specifying the source and destination; 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 the rules.
- Keywords (in a domain name or 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 a port number.
- Reports and alerts that you want the router to send to you.

You can, for example, establish restricted-access policies based on the 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 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, by 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.

Basic Firewall Settings

To configure basic firewall settings:

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

STEP 2 Configure the following firewall settings:

SPI Firewall	Check **Enable** to enable the firewall.
DoS Protection	Check **Enable** to enable Denial of Service protection.
Block Ping WAN Interface	Check **Enable** to block ping WAN interface.
SSH Access	Check **Enable** to enable SSH access.
Remote SSH Access	Check **Enable** to enable remote SSH access.

Web Access	Select the type of web access that can be used to connect to the firewall: HTTP or Redirect HTTP traffic to HTTPS or HTTPS (secure HTTP).
Remote Web Access	Check **Enable** to enable remote web access and select connection either HTTP or HTTPS.
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**
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.
Unicast RPF	Unicast Reverse Path Forwarding (Unicast RPF) can help limit the malicious traffic on an enterprise network. It works by verifying the reachability of the source address in the packets being forwarded. It can limit the appearance of spoofed addresses on a network. If the source IP address is not valid, the ticket is discarded. In the RV132W/RV134W, the Unicast RPF works in strict mode or loose mode. In strict mode, the packet must be received on the interface that the router would use to forward the return packet. In loose mode, the source address must appear in the routing table. In the Unicast RPF select one of the following from the drop down list (**Disable unicast, Strict unicast** or **Loose unicast**).

SIP ALG	Check **Enable** to allow Session Initiation Protocol (SIP) traffic to traverse the firewall.
UPnP	Check **Enable** to enable UPnP.
Allow Users to Configure	Check **Enable** 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 **Enable** to allow users to disable Internet access.
Block Java	Check to block Java applets. Java applets are small programs embedded in web pages that enable the 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 the websites that usually require a 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 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**.

CAUTION When remote web 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.

Schedule Management Configuration

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 Select **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 **Access Rules Configuration**.)

STEP 4 In the **Scheduled Days** section, select if you want to apply the schedule to All Days or Specific Days. If you select **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, select the time when you want the schedule to apply. If you select **Specific Time**, enter the start and end times.

STEP 6 Click **Save**.

Services Management Configuration

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 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 Select **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, select the Layer 4 protocol that the service uses from the drop-down list:

- **TCP**
- **UDP**
- **TCP & UDP**
- **ICMP**
- **ICMPv6**
- **Other**

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 If you select the ICMP Type field, enter the ICMP protocol type.

STEP 8 If you select the other protocol, enter the protocol number.

STEP 9 Click **Save**.

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

Access Rules Configuration

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 Select **Firewall** > **Access Rules**.

STEP 2 Select **Allow** or **Deny**.

NOTE Ensure that IPv6 support is enabled on the device to configure an IPv6 firewall.

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 Select **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 Select **Firewall > Access Rules**.

STEP 2 Click **Add Row**.

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

- **Outbound (LAN > WAN)** - Select this option to create an outbound rule.
- **Inbound (WAN > LAN) -** Select this option to create an inbound rule.
- **Inbound (WAN > DMZ) -** Select this option to create an inbound rule.
- **Inter-VLAN (VLAN > VLAN)** - Select this option to create an inter-VLAN rule.
- **Inter-VLAN (VLAN >DMZ)** - Select this option to create an inter - VLAN rule.

STEP 4 From the **Action** drop-down list, select 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 list, select the service to allow or block for this rule. Select **All Traffic** to allow the rule to apply to all applications and services, or select a single application to block:

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

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

STEP 6 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 From the **Source IP** drop-down list choose the source IP addresses to which the rule blocks or allows packets from.

- **Any** — The rule applies to all source IP addresses.
- **Single Address** — Enter a single IP address to which the rule applies in the Start field.
- **Address Range** — Enter a range of IP addresses to which the rule applies to in the Start and Finish fields

STEP 8 From the **Destination IP** drop-down list choose the destination IP addresses to which the rule blocks or allows packets to.

- **Any** — The rule applies to all destination IP addresses.
- **Single Address** — Enter a single IP address to which the rule applies to in the Start field.

- **Address Range** — Enter a range of IP addresses to which the rule applies to in the Start and Finish fields

STEP 9 To log details for all packets that match this rule, select **Always** from the drop-down list. 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.

Select **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 10 **Rule Status -** Check **Enable** to enable the new access rule.

STEP 11 Click **Save**.

Internet Access Policy Configuration

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 an Internet access policy:

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

STEP 2 Click **Add Row**.

STEP 3 Check **Status Enable**.

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

STEP 5 From the **Action** drop-down list, select 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 **Schedule Management Configuration**.

STEP 6 Select a schedule from the drop-down list.

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 list, select 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 list, select 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 **Domain Name, URL** or **Keyword** used to block the website.

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

STEP 9 Click **Save**.

One-to-One NAT Configuration

Use the One-to-one Network Translation (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 Select **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, select 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.**

Single Port Forwarding Configuration

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.To add a single port forwarding rule:

STEP 1 Select **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 From the **Protocol** drop-down list, select a protocol (**TCP, UDP**, or **TCP** & **UDP**)

STEP 6 In the **Interface** drop-down list, select **DSL_ATM_WAN, DSL_PTM_WAN, ETH_WAN, or USB_WAN**.

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 the 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**.

Port Range Forwarding Configuration

To add a port range forwarding rule:

STEP 1 Select **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 **Start** field, specify the port number that begins the range of ports to forward.

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

STEP 5 From the **Protocol** drop-down list, select a protocol (**TCP**, **UDP**, or **TCP** & **UDP**)

STEP 6 In the **Interface** drop-down list, select **DSL_ATM_WAN, DSL_PTM_WAN, ETH_WAN, or USB_WAN**.

STEP 7 In the **IP Address** field, enter the IP address of the host on the LAN side to which the specific IP traffic will be forwarded.

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

STEP 9 Click **Save**.

Port Range Triggering Configuration

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 Select **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 list, select **DSL_ATM, DSL_PTM, ETH_WAN,** or **USB_WAN.**

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

STEP 7 Click **Save**.

Attack Protection Configuration

Use the **Attack Protection** page to specify how to protect your network against common types of attacks including discovery, flooding, and echo storms.

STEP 1 Click **Firewall > Attack Protection**.

STEP 2 Check the following and enter a numeric range for each:

- **SYN Flood Detect Rate:** Enter the maximum number of SYN packets per second that will cause the security appliance to determine that a SYN Flood Intrusion is occurring. Enter a value from 0 to 10000 SYN packets per second. The default value is 128 SYN packets per seconds. A value of zero (0) indicates that the SYN Flood Detect feature is disabled.
- **Echo Storm:** Enter the number of pings per second that will cause the security appliance to determine that an echo storm intrusion event is occurring. Enter a value from 0 to 10000 ping packets per second. The default value is 100 ping packets per seconds. A value of zero (0) indicates that the Echo Storm feature is disabled.

- **ICMP Flood**: Enter the number of ICMP packets per second, including PING packets, that will cause the security appliance to determine that an ICMP flood intrusion event is occurring. Enter a value from 0 to 10000 ICMP packets per second. The default value is 100 ICMP packets per seconds. A value of zero (0) indicates that the ICMP Flood feature is disabled.
- **Block UDP Flood:** Check to prevent the security appliance from accepting more than 150 simultaneous, active UDP connections per second from a single computer on the LAN and enter a value from 0 -10000, default = 1000.
- **Block TCP Flood**: Check to drop all invalid TCP packets and enter a value from 0 - 10000, default = 200. This feature protects your network from a SYN flood attack, in which an attacker sends a succession of SYN (synchronize) requests to a target system.

STEP 3 Click **Save**.

Session Settings Configuration

You can limit the maximum number of unidentified sessions and half-open sessions on the Cisco RV132W/RV134W. You can also introduce timeouts for TCP and UDP sessions to ensure Internet traffic is not deviating from expectations in your private network.

To configure session settings:

STEP 1 Select **Firewall > Session Setting**.

STEP 2 In the **TCP Session Timeout** field, enter the time, in seconds, after which inactive TCP sessions are removed from the session table. Most TCP sessions normally terminate when the RST or FIN flags are detected. This value ranges from 18000 through 432000 seconds. The default is 86,400 seconds (24 hours).

STEP 3 In the **UDP Timeout** field, enter the time, in seconds, after which inactive UDP sessions are removed from the session table. This value ranges from 90 through 360 seconds. The default is 180 seconds (3 minutes).

STEP 4 In the **ICMP Timeout** field, enter the time, in seconds, after which inactive ICMP sessions are removed from the session table. This value ranges from 15 through 60 seconds. The default is 30 seconds.

6

VPN

Site-to-Site IPsec VPN

Site-to-site VPNs are implemented based on the IPsec policies that are assigned to the VPN topologies. An IPsec policy is a set of parameters that define the characteristics of the site-to-site VPN, such as the security protocols and algorithms that will be used to secure traffic in an IPsec tunnel.

Configuring Basic VPN Setup

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, which will be exchanged between the two routers. It must be between 8 and 49 characters.

STEP 4 In the **Protocol** field select the protocol name from the drop-down menu

STEP 5 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**— Is generated automatically.
- 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 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.

NAT Traversal

Network address translation (NAT) traversal is a computer networking methodology with the goal to establish and maintain Internet protocol connections across gateways that implement network address translation (**NAT**).

STEP 1 To enable NAT traversal, in the **NAT Traversal** field, check **Enable.**

Managing IKE Policies

The Internet Key Exchange (IKE) protocol dynamically exchanges keys between two IPsec gateways. 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, in the IKE Policy Table click **Add Row**.

STEP 2 In the **Policy Name** field, enter a unique name for the IKE policy.

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 one of the following:

- Local WAN IP: the WAN IP address
- IP Address: use a user defined IP address as an ID
- FQDN: use a Fully Qualified Domain Name as an ID
- USER FQDN: the email address or other ID.
- DER ASN1 DN: the Distinguished Name of the certificate. When you choose this option, please input the Subject Name of the device certificate. The string format is “C=US/ST=sjc/L=cisco/0=cisco/OU=smb/CN=RV134W”.

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.

- In the **Authentication Method** field, select one of the following options:
- **Pre-Shared Key**: the VPN peers use a pre-shared key to authenticate each other.
- **Certificate**: the VPN peers use a certificate to authenticate each other. When the Authentication Method is Certificate:
  - The Local/Remote Identifier can be set to “DER ASN1 DN” with the value of the Distinguished Name of the certificate.
  - The Local/Remote Identifier can also be set to one of Local WAN IP, FQDN, USER FQDN, as long as the SubjectAltName of the certificate has the same type/value as the Identifier. That also means if the CSR of the certificate is generated by the device (under the menu VPN > Site-to-Site IPSec VPN > Certificate Management > Generate CSR), the “IP Address”, “Domain Name”, or “Email Address” should be filled with the correct value.

c. 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.

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

e. 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 at every interval.
- **Failure Count**—This field shows the number of failure counts. The default setting is 3. The device will consider the peer is dead if it does not receive DPD response from the peer for this number of times.

- **DPD Action** - Select Terminate if you want to end the session or Reconnect to reconnect.

f. **Extended Authentication** - To enable XAUTH.

STEP 6 Click **Save.**

NOTE (For RV132W only) 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**. In the VPN Policy Table, 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. **VPN Failover** — Check **Enable** to enable VPN failover. If enabled, the “Interface” configuration will gray out. The VPN tunnel will always build on the active WAN interface.

d. **Interface**—Select which WAN interface the VPN tunnel is on.

e. **Redundant Enable** — With Redundant Enable selected, if the device fails to establish the tunnel with the “Remote Endpoint”, (configured on the same page), it will try to establish the tunnel with the “Redundant Remote Endpoint”.

f. **Redundant Remote Endpoint—**Select the type of identifier that you want to provide for the gateway at the remote endpoint: **IP address** or **FQDN**. Enter the IP address or the FQDN.

g. **Redundant Remote Identifier Type**—Select the redundant remote identifier type from the drop down list: **Local Wan IP, IP Address, FQDN, User-FDQN**, or **DER ASN1 DN.**

STEP 3 **NetBIOS**: Computers running Microsoft Windows® communicate with one another through NetBIOS broadcast packets. Enable NetBIOS to access remote network resources by browsing the Windows® Network Neighborhood.

STEP 4 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 5 **Split DNS**—Allow the router to find the DNS server of the remote router without going through the ISP (Internet). If you enable Split DNS, also enter these settings: Domain Name Server 1-2, Domain 1-6. Domain Name Server1-2 will resolve the Domain Name 1-6.

STEP 6 **Manual Policy Parameters**—For a **Manual** policy type, enter the settings in the **Manual Policy Parameters** section:

- **Protocol** —Select the protocol from the drop down list: **ESP** or **AH.**
- **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.
- **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:
  - 3DES—24 characters
  - AES-128—16 characters
  - AES-192—24 characters
  - AES-256—32 characters
- **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
  - None, SHA2-384, SHA2-512

STEP 7 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 30 seconds.

- **Protocol**—Select the protocol from the drop down list: **ESP** or **AH**
- **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 8 Click **Save**.

Configuring Hub and Spoke

In a VPN hub-and-spoke topology, multiple VPN routers (spokes) communicate secure with each other via a central VPN router (hub). A separate, secured tunnel extends between each individual spoke and the hub.

TIP You may find it helpful to create a worksheet listing the LAN IP address, LAN subnet, and netmask for each site, When configuring at a spoke site, you will need the network addresses of the main site and all other spoke sites. When configuring the at the hub site, you will need the network addresses of all of the spoke sites.

Hub	Spoke1	Spoke2
192.168.1.100	192.168.75.100	192.168.74.100
192.168.1.0	192.168.75.0	192.168.74.0
255.255.255.0	255.255.255.0	255.255.255.0

Configuring the Hub Site

When configuring the hub site, you will create two VPN policies for the hub site at the same time, for example VPN policy HubToSpoke1 andHubToSpoke2 at the same time. To configure the hub enter the following information:

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

STEP 2 To configure the VPN settings for hub site, configure the following features:

Add/Edit VPN Policy Configuration > Policy Name	Enter **HubToSpoke1** or **HubToSpoke2**
Policy Type	Select **Auto Policy** from the drop-down list.
VPN Failover	Leave unchecked.
Interface	Select the Internet interface from drop-down list.

Remote Endpoint	Select **IP Address** from the drop-down list and enter the IP address.
Redundant Enable	Leave unchecked.
NetBIOS	Leave unchecked.
Local Traffic Section > Local IP	Select **Subnet** from the drop-down list.
IP Address	Enter the local LAN subnet, for example, **192.168.1.0** and **192.168.74.0** for HubToSpoke1 or **192.168.1.0** and **192.168.75.0** for HubToSpoke2.
Subnet Netmask	Enter **255.255.255.0,** then click Add to enter the address in the **IP/Subnet List**.
Remote Traffic Section >Remote IP	Select Subnet from the drop-down list.
IP Address	Enter remote LAN subnet, for example **192.168.75.0** for HubToSpoke1 or **192.168.74.0** for HubToSpoke2.
Subnet Netmask	Enter **255.255.255.0,** then click Add to enter the address in the **IP/Subnet List.**

STEP 3 Click **Save.**

Configuring the Spoke Site

When configuring the spoke site, you will create a VPN policy for each spoke site, for example, VPN policy Spoke1ToHub for spoke site1 and Spoke2ToHub for spoke site2. To configure the spoke site enter the following information:

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

To configure the VPN settings for each spoke site, configure the following features:

Add/Edit VPN Policy Configuration > Policy Name	Enter **Spoke1ToHub** or **Spoke2toHub**.
Policy Type	Select **Auto Policy** from the drop-down list.
VPN Failover	Leave unchecked.

Interface	Select the Internet interface from drop-down list.
Remote Endpoint	Select **IP Address** from the drop-down list and enter the IP address.
Redundant Enable	Leave unchecked.
NetBIOS	Leave unchecked.
Local Traffic Section > Local IP	Select **Subnet** from the drop-down list.
IP Address	Enter local LAN subnet, for example **192.168.75.0** for Spoke1ToHub or **192.168.74.0** for Spoke2ToHub.
Subnet Netmask	Enter **255.255.255.0,** then click Add to enter the address in the **IP/Subnet List**.
Remote Traffic Section >Remote IP	Select **Subnet** from the drop-down list.
IP Address	Enter remote LAN subnet, for example **192.168.1.0 and 192.168.74.0** for Spoke1ToHub or **192.168.1.0** and **192.168.75.0** for Spoke2ToHub.
Subnet Netmask	Enter **255.255.255.0,** then click **Add** to enter the address in the **IP/Subnet List.**

STEP 2 Click **Save.**

STEP 3 Now the subnet 192.168.75.0/24 on Spoke1 can communicate with subnet 192.168.74.0/24 on Spoke2 via Hub.

Certificate Management

A digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or assertions made by the private key that corresponds to the public key that is certified. In this model of trust relationships, a CA is a trusted third party that is trusted by both the subject (owner) of the certificate and the party relying upon the certificate. CAs are characteristic of many public key infrastructure (PKI) schemes.

The table has a self-signed local certificate by default. All imported CA certificates and local certificates, as well as the generated CSR, are also shown in the table. The default local certificate is self-signed, and may be exported, but not deleted. It is used only by HTTPS GUI access. All other local certificates can be deleted and exported. The CA certificates can be deleted but not exported. The CSRs can be deleted and exported. The “Action” column also has an “Import” button for the CSRs. It is used to import the local certificate that the CA issues based on this CSR.

Use Certificate Management to generate and install SSL certificates.

To import a certificate:

STEP 1 Select **VPN > Certificate Management**. In the **Certificate Management** table, click **Import Certificate**.

STEP 2 Select **Import CA** or **Import Local Certificate**.

STEP 3 Browse and locate certificate. The RV132W/RV134W only support PEM format certificate. Please make sure the certificate format is PEM and file extension name is .pem.

STEP 4 Click **Start Upload.**

STEP 5 Click **Save.**

Certificate Generator

The Certificate Request Generator collects information and generates a private key file and a certificate request. You can choose to generate a self-signed certificate or a Certificate Signing Request (CSR) for an external certificate authority to sign.

To generate a certificate:

STEP 1 Select **VPN > Certificate Management**. In the **Certificate Management** table, click **Generate CSR**.

STEP 2 Enter the following parameters:

- **Certificate Name**—Name of certificate.
- **Country Name**—Country of origin.
- **State or Province Name**—State or province (optional).
- **Locality Name**—Municipality (optional).
- **Organization Name**—Organization (optional).
- **Organizational Unit Name**—Subset of the organization.
- **Common Name**—Common name of the organization.
- **Key Encryption Length**—Length of the key.
- **IP Address**—IP address (optional). If you want to use the Local WAN IP as the Local Identifier, enter the value of the Local WAN IP here.
- **Domain Name**—Name of the domain (optional). If you want to use FQDN as the Local Identifier, enter the value of FQDN here.
- **Email Address**—Contact email address (optional). If you want to use the User FQDN as the Local Identifier, enter the value of the User FQDN here.

STEP 3 Click **Save**.

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 (For the RV134W only):

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

STEP 2 In the PPT Configuration, enter the following information.

a. In the PPTP Server field, check **Enable**.

b. Enter the IP address for 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 **Enable** to enable **MPPE Encryption**. The MPPE encryption for the PPTP server support is 128 bit.

STEP 3 Click **Save**.

Creating and Managing PPTP Users

To create and enable PPTP users:

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

STEP 2 Enter the username and password that will authenticate the PPTP user. Enter values that are between 1 to 64 characters long.

STEP 3 Check **Enable** to enable the user account.

STEP 4 Click on the Import button to access the user configuration page (under menu Administration > Users). At the bottom of the page, import the.csv file with the username/password pairs.

STEP 5 Click **Save.**

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

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.

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 bandwidths of the Internet link.

To set the upstream bandwidth:

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

STEP 2 In the Global Settings, in the WAN QoS field, check **Enable**.

STEP 3 In the **Bandwidth Table**, enter the upstream bandwidth you want to allocate to each of the available interfaces.:

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

STEP 4 Click **Save**.

Configuring QoS Binding Policy

In the QoS Binding Table, you can configure QoS policy for upstream traffic.

STEP 1 Click **Add Row**.

STEP 2 Enter information in the following fields to add or edit policy settings:

Policy Name	Name of policy.
Protocol	Select the protocol from the drop-down list. (TCP & UCP, TCP or UCP).
Source Port	Select the source port from the drop down list. It can be any port, a single port or port range.
Destination Port	Select the destination port from the drop down list. It can be any port, a single port or port range.
Source IP	Select the source IP from the drop down list. It can be any IP address, a single IP address or an IP address range.
Destination IP	Select the destination IP from the drop down list. It can be any IP address, a single IP address or an IP address range.
MAC Address	Select the type of MAC address from the drop down list. It can be **Any** or **Single MAC** address. This is the MAC address of the source of this traffic.
VLAN ID	Select the **VLAN ID** from the drop-down list. This is the VLAN ID of the source of this traffic.
Available SSIDs	Select the available **SSIDs** from the drop-down list. This is the SSID of the source of this traffic.
Physical Port	Select the port (**1 -3 for RV132W** or **1- 4 for RV134W**) from the drop-down list. This is the LAN port of the source of this traffic.
Queue	Set the priority (**1 lowest to 4 highest)** for the selected category.
Rate Limit (Kbit/Sec):	Enter the rate limit in Kbits per second.

Remarking	Check **Enable** to enable remarking on the Class of Service (CoS) or Differentiated Services Code Point (DSCP).
CoS or 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**.

Configuring QoS Port-Based Settings

You can configure QoS settings for every port on your device. It supports four priority queues that allow traffic prioritization for each port.

To configure QoS settings for the ports on your device:

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

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

Trust Mode	Select 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 4. • **DSCP**—Differentiated Services Code Point (DSCP). Enabling this feature prioritizes the network traffic based on the DSCP queue mapping on the **DSCP Settings** page. • **CoS**—Class of service (CoS). Enabling this feature prioritizes the network traffic based on the CoS queue mapping on the **CoS Settings** page.
Default Traffic Forwarding Queue for Untrusted Devices	Select a priority level for outbound traffic (1 to 4).

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 Select **QoS** > **CoS Settings**.

STEP 2 For each CoS priority level in the **CoS Settings Table**, select 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 Select **QoS** > **DSCP Settings**.

STEP 2 Select whether only to 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**, select 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

Administration

Password Complexity

Password strength and complexity is a preventative measure used in resisting guessing and brute-force attacks. The strength of a password is a function of length, complexity, and unpredictability.

Using strong passwords lowers overall risk of a security breach. You can enforce a minimum password complexity requirement for password changes.

To configure password complexity settings:

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

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

STEP 3 Configure password complexity settings:

Minimum password length	Enter the minimum password length (0-32 characters).
Maximum password length	Enter the maximum password length (64-80 characters)
Minimum number of character classes	Enter a number representing one of the following character classes: • Uppercase letters. • Lowercase letters. • Numbers. • Special characters are available on a standard keyboard. By default, passwords must contain characters from at least three of these classes.

The new password must be different than the current one	Check **Enable** to require that new passwords differ from the current password.
Enforce Password Aging	Check **Enable** to expire passwords after a specified time.
Maximum Password Age	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.

Configuring User Accounts

To configure the user accounts:

STEP 1 Select **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 recommend 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

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**.

STEP 4 Click **Save**.

NOTE You may download the user template to create your own list of user name and passwords. To download the template, click **Download** in the **Download User template** field.

Session Timeout Configuration

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

To configure session timeout:

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

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

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

STEP 4 In the **SSH Inactivity Timeout** field, enter the number, in minutes, before a session times out due to inactivity. Select **Never** to allow the administrator to stay logged in permanently

STEP 5 Click **Save**.

Login Banner Text

Login banners (for command line interface [CLI] only) provide a warning to intruders that may want to access your system. They confirm that certain types of activities are prohibited and advise the authorized users of their obligations relating to the acceptable use of the networked environment(s).

To update the **Pre-Login Banner Text** fields enter the login banner text in the text box. It is displayed on the CLI before user login.

To update the **Post-Login Banner Text** fields, enter the login banner text in the text box. It is displayed on the CLI after user login.

Configuring TR-069 Settings

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

NOTE The TR069 and GUI management can not work simultaneously. After configuring the TR069 and saving the settings, logout of the web GUI. Thereafter, the CPE can initiate the connection to the ACS.

To configure the TR-069 settings:

STEP 1 Click Administration > **TR-069 Settings**. The **TR-069 Settings** page opens.

STEP 2 In the **TR-069 Settings** area, click **Enable** to enable the TR-069 client, or click **Disable** to disable it.

STEP 3 In the **IP Protocol** area, check **IPv4** or **IPv6** protocol.

STEP 4 In the **Inform** area, check **Enable** to enable Inform or **Disable** to disable it.

STEP 5 In the **Inform Interval** field, enter the number in seconds (Default setting is 300).

STEP 6 In the **ACS** area, specify the settings of the ACS remote management server:

- **ACS URL:** Click the ACS URL drop down list to choose ACS URL protocol - HTTP:// or HTTPS:// and enter the URL.
- **ACS Username:** Enter the username to log in to the ACS remote management server.
- **ACS Password:** Enter the password to log in to the ACS remote management server.
- If the https protocol is selected, complete the following:
- **ACS side CA certificate file import:** Click to import trusted CA certificate file content.

- **ACS side CA certificate file show**: Click to show trusted CA certificate list.
- **ACS certificate file select**: Click to select drop down list of trusted CA.
- **CPE certificate file import**: Click to import CPE CA certificate file content.
- **CPE certificate file show**: Click to show CPE CA certificate list.
- **CPE certificate file select**: Click to select drop down list of CPE CA.

STEP 7 In the **Display SOAP messages on the serial console,** check **Enable** to display SOAP messages or **Disable** to disable it.

STEP 8 **Download Request:** (Optional) Specify the type of download request and then click **Send** to send the corresponding download request to the TR-069 server.

- **Firmware:** Request to download the firmware of the RV132W/RV134W from the TR-069 server.
- **Vendor Configuration:** Request to download the configuration file from the TR-069 server.

STEP 9 Check **Connection Request Authentication** and enter the following information:

- **Username:** Enter the username to log in using the connection request authentication.
- **Password:** Enter the password to log in using the connection request authentication.
- **Connection Request port**: Enter the port for connection request. It's 7547 by default.

STEP 10 In the **Bind Interface** field, select **Auto** to bind the TR-069 service with the current active interface, or select one of the interfaces to bind it with. Click **Save** to save your settings.

STEP 11 Click **Export Data Model** to export the TR-069 model of the device.

Diagnostics

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

Network Tools

Use the following diagnostic utilities to access the configuration of the RV132W/ RV134W and monitor the overall network health.

Using Ping or Trace

You can use the Ping or Trace utility to test connectivity between this router and another device in the network. To use Ping or Trace:

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. Or click **Traceroute**. The Traceroute results appear.

Performing a DNS Lookup

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

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

To use the Lookup tool:

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

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

STEP 3 Click **Look up**. The DNS lookup results appear.

Packet Capture

Packet capture is a computer networking term for intercepting a data packet that is crossing or moving over a specific computer network.

To start a packet capture, from the **Select a layer 2 interface for this service** drop-down menu select your connection type (LAN, DSL WAN or ETH WAN).

- Click **Start** to start the packet capture.
- Click **Stop** to stop the packet capture.
- Click **Save packet log** to save the packet log.

STEP 4 **DSL Diagnostics**. Click **Enable** to enable the DSL Diagnostics.

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, 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 Select **Administration** > **Diagnostics** > **Port Mirroring**.

STEP 2 From the **Mirror Destination Port** drop-down menu, select a mirror port. If you use a port for mirroring, do not use it for any other traffic.

STEP 3 In the **Mirror Source Port** field, select the ports to mirror.

STEP 4 Click **Save**.

Remote Support Key Settings

The support key is used by Cisco support engineers to get more information on the device during troubleshooting. The default key is "**key001**". Please include the key when you open a support case with Cisco and want the support engineer to access your device remotely. To setup a remote support key, enter the name of the key in the **Remote Support Key** field.

Logging Configuration

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

Configuring Log Settings

To configure logging:

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

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

STEP 3 Click **Add Row**.

STEP 4 Configure the following settings:

Remote Log Server	Enter the IP address of the log server that will maintain logs.
Log Severity	Select the severity of events for which you want to maintain and send logs to a specific server/email address. All log types that are higher in severity than the selected log type are automatically included and cannot be excluded. For example, if you select Error logs, Emergency, Alert, and Critical are also selected. The event severity levels are listed from the highest to the lowest: • **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	Check **Enable** to enable the logging settings.

STEP 5 Click **Save.**

STEP 6 Click **View Logs** to view the system log table.

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

Configuring E-Mail Settings

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 Select **Administration** > **Logging** > **E-mail Settings**.

STEP 2 To enable E-mail logs, check **Enable**.

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

STEP 3 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, (Address 2, optional), (Address 3, optional)	Enter an email address to which to send logs (for example, logging@companyname.com).
E-mail Encryption	Select **SSL** or **TSL** as the email encryption method. Select **Enable** to use an email encryption method.
Authentication with SMTP Server	If the SMTP (mail) server requires authentication before accepting connections, select 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 Test	Click **Test** to test email authentication.

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

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

STEP 5 In the Email Alert section, configure the following settings:

Email alert when WAN up/down	Check **Enable** to receive an email alert when the WAN is up or down.
Email alert when VPN up/down	Check **Enable** to receive an email alert when the VPN is up or down.

STEP 6 Click **Save**.

Discovery Bonjour Configuration

Discovery 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 Discovery Bonjour:

STEP 1 Select **Administration** > **Discovery 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 on the VLAN to discover the 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 on the VLAN 2 cannot discover the Bonjour services running on the router unless Bonjour is enabled for VLAN 2.

STEP 4 Click **Save**.

LLDP Properties Configuration

LLDP is a neighbor discovery protocol that is used for network devices to advertise their information to other devices on the network. This protocol runs over the data-link layer, which allows two systems running different network layer protocols to learn about each other.

To enable LLPD properties on the router, follow these steps:

STEP 1 Select **Administration >LLDP Properties.**

STEP 2 Check **Enable** to enable the following: LLPD status, DSL_ATM_WAN_0_33_R, ETH_WAN_R, DSL_PTM_WAN_1_1_R, IP_USB, PPP_USB.

STEP 3 Click **Save.**

Time Settings Configuration

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 Select **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.
Daylight Saving Mode	If you select **By date**, enter the specific date when daylight saving mode starts. If you select **Recurring**, enter the month, week, the day of the week, and time when daylight saving time starts. Enter the appropriate information in the **From** and **To** fields.

Daylight Saving Offset	Select 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 to set manually or automatically.
NTP Server	To use the default NTP servers, click the **Use Default** button. To use a specific NTP server, click the **User Defined NTP Server** and enter the fully qualified domain name or IP address of the NTP servers in the two available fields.
Enter Date and Time	If you select **Manual,** enter the date and time in the **Enter Date and Time** fields.

STEP 3 Click **Save**.

Download and Backup Configuration File

You can back up custom configuration settings for future restoration or restore them from a previous backup from the **Administration > Download /Backup Configuration File** page.

When the firewall is working as configured, you can back up the configuration for future restoration. 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 Select **Administration** > **Download/Backup Configuration Settings**.

STEP 2 Select the configuration from the **Configuration Download & Clear** settings:

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 RV132/RV134W 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**.

Configuration Upload

To upload a startup or backup configuration:

STEP 1 Select **Administration >Download/Backup Configuration File**.

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 Select **Administration > Download/Backup Configuration File.**

STEP 2 In the **Copy** field, select 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 Select **Administration > Download/Backup Configuration File.**

STEP 2 Click **Show Advanced Settings**.

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

STEP 4 Click **Save**.

Firmware Upgrade

You can upgrade to a newer version of the firmware for the router by using the **Administration > Firmware Upgrade** page.

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

Upgrading Firmware

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

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

STEP 2 In the **Firmware Upgrade** section, click **Download** to download the latest version of the firmware.

STEP 3 You can also upgrade the firmware by clicking on **Browse** to locate and upload the latest firmware files from a specific location:

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

CAUTION Resetting the device to factory default 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.

Firmware Recovery Steps

If the firmware corrupts during the upgrade or a power outage, the PWR LED light will turn red. Please follow these steps to upload and recover the firmware.

STEP 1 Power off the router.

STEP 2 There are 2 ways to access the firmware recovery mode. You can select any of the following options to access the recovery mode.

- If the firmware is corrupt and the router is unable to boot normally, the router will automatically go into recovery mode after the device is powered on. The PWR LED will turn red. Usually, the original configuration will be restored after the new firmware is uploaded.
- To enter the recovery mode manually, connect the console cables (baud rate 115200)to the router. Power on the router and the boot up log will be displayed on the console terminal. Press any key to stop the normal startup. The PWR LED will turn red. Usually, the original configuration is restored after the new firmware is uploaded.
- To delete the original configurations on the router, press the reset button and power on the router.

STEP 3 Connect the PC to the LAN1 port. Configure the PC's static address as 192.168.1.100.

STEP 4 Recover the firmware to the router via Web UI. For example, you can enter "http://192.168.1.1" in the browser, then choose the image like (for RV132W) "RV132W_FW_ANNEX_A_1.0.0.10.bin" or (for RV134W) "RV134W_FW_ANNEX_A_1.0.0.10.bin", and press Recover & Reboot. Wait for several minutes until the router reboots itself once the upload is completed and is flashing.

STEP 5 After the router will starts up normally, the PWR will be on and green.

Reboot

To reboot the router:

STEP 1 Select **Administration** > **Reboot**.

STEP 2 Check **Reboot the device**.

STEP 3 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 Select **Administration** > **Reboot**.

STEP 2 Check **Return to factory default settings after reboot.**

STEP 3 Click **Reboot**.

9

Where to Go From Here

Support	
Cisco Support Community	www.cisco.com/go/smallbizsupport
Cisco Support and Resources	www.cisco.com/go/smallbizhelp
Phone Support Contacts	www.cisco.com/en/US/support/tsd_cisco_small_ business_support_ center_contacts.html
Cisco Firmware Downloads	www.cisco.com/go/smallbizfirmware Select a link to download firmware for Cisco products. No login is required.
Cisco Open Source Requests	If you wish to receive a copy of the source code to which you are entitled under the applicable free/open source license(s) (such as the GNU Lesser/General Public License), please send your request to: external-opensource-requests@cisco.com In your requests please include the Cisco product name, version, and the 18 digit reference number (for example: 7XEEX17D99-3X49X08 1) found in the product open source documentation.
Cisco Partner Central (Partner Login Required)	www.cisco.com/web/partners/sell/smb
Cisco RV134 Wireless Multifunction VPN Router	www.cisco.com/en/US/products/ps9923/tsd_products_support_series_home.html