THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)
Introduction

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.
IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)
CONTENTS

Full Cisco Trademarks with Software License  iii

Introduction  iv

CHAPTER 1  Getting Started  1
  Setting Up Your Device  1
  Getting Started  3
  Troubleshooting Tips  4
  User Interface  4

CHAPTER 2  Status and Statistics  7
  System Summary  7
  TCP/IP Services  9
  Port Traffic  10
  WAN QoS Statistics  11
  ARP Table  11
  Routing Table  12
  DHCP Bindings  12
  Mobile Network  13
  View Logs  13
  Captive Portal Status  14

CHAPTER 3  Administration  17
  File Management  17
WAN Settings 41
Multi-WAN 44
Mobile Network 45
  Mobile Network Setup 46
  Bandwidth Cap Setting 46
Dynamic DNS 47
Hardware DMZ 47
IPv6 Transition 48
  IPv6 in IPv4 Tunnel (6in4) 48
  IPv6 Rapid Deployment (6rd) 48

CHAPTER 6  LAN 51
  Port Settings 51
  VLAN Settings 52
  LAN/DHCP Settings 53
  Static DHCP 55
  802.1X Configuration 55
  DNS Local Database 56
  Router Advertisement 56

CHAPTER 7  Wireless (RV340W) 59
  Basic Settings 59
    Configuring 2.4 GHz Radio 61
    Configuring 5 GHz Radio 62
  Advanced Settings 62
  Captive Portal 63
  WPS 65

CHAPTER 8  Routing 67
  IGMP Proxy 67
  RIP 68
  Static Routing 69

CHAPTER 9  Firewall 71
Getting Started

Thank you for choosing the Cisco RV340. This guide describes how to install and manage your device. Your Cisco RV340 comes with default settings. However, your internet service provider (ISP) might require you to modify the settings. You can modify the settings using a web browser such as Internet Explorer (version 10 and higher), Firefox, or Chrome (for PC) or Safari (for Mac).

Thank you for choosing the Cisco RV340W. This guide describes how to install and manage your device. Your Cisco RV340W comes with default settings. However, your internet service provider (ISP) might require you to modify the settings. You can modify the settings using a web browser such as Internet Explorer (version 10 and higher), Firefox, or Chrome (for PC) or Safari (for Mac).

This section contains the following topics:
- Setting Up Your Device, on page 1
- User Interface, on page 4

Setting Up Your Device

This section will help get you started with your device by following these steps:

**Step 1**
Connect a PC to a numbered LAN port on the device. If the PC is configured to become a DHCP client, an IP address in the 192.168.1.x range is assigned to the PC.

**Step 2**
Start a web browser.

**Step 3**
In the address bar, enter the default IP address of the device, **192.168.1.1**. The browser might issue a warning that the website is untrusted. Continue to the website.

**Step 4**
When the sign-in page appears, enter the default username cisco and the default password cisco (lowercase).

**Step 5**
Click **Login**.

**Note**
During the system boot up, the power LED will progressively keep flashing until the system has fully booted.

At start up, the PWR, LINK/ACTION and GIGIBIT LEDs of LAN 1 will flash. At 25% boot up, the PWR, LINK/ACTION and GIGIBIT LEDs of LAN 1 and 2 will flash. At 50% boot up, the PWR, LINK/ACTION and GIGIBIT LEDs of LAN 1, 2 and 3 will flash. At 75% boot up, the PWR, LINK/ACTION and GIGIBIT LEDs of LAN 1, 2, 3 and 4 will flash.

The system boot time will be less than 3 minutes typically. If the device is fully configured with all feature configuration settings set to a maximum, it may take up to 7 minutes to fully boot the system.
Table 1: Description of the LEDs

<table>
<thead>
<tr>
<th>LED</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PWR</td>
<td>Off when the device is powered off.</td>
</tr>
<tr>
<td></td>
<td>Solid green when the device is powered on and booted.</td>
</tr>
<tr>
<td></td>
<td>Flashing green when the device is booting up.</td>
</tr>
<tr>
<td>DIAG</td>
<td>Off when the system is on track to bootup.</td>
</tr>
<tr>
<td></td>
<td>Slow blinking red (1Hz) when the firmware upgrade is in progress.</td>
</tr>
<tr>
<td></td>
<td>Fast blinking red (3Hz) when the firmware upgrade is failing.</td>
</tr>
<tr>
<td></td>
<td>Solid red when the system failed to boot-up with both active and inactive images or in rescue mode.</td>
</tr>
<tr>
<td>LINK/ACT of WAN1, WAN2 and LAN 1-4</td>
<td>Off when there is no Ethernet connection.</td>
</tr>
<tr>
<td></td>
<td>Solid green when the GE Ethernet link is on.</td>
</tr>
<tr>
<td></td>
<td>Flashing green when the GE is sending or receiving data.</td>
</tr>
<tr>
<td>GIGABIT of WAN1, WAN2 and LAN 1-4</td>
<td>Solid green when at 1000M speed.</td>
</tr>
<tr>
<td></td>
<td>Off when at non-1000M speed.</td>
</tr>
<tr>
<td>DMZ</td>
<td>Solid green when the DMZ is enabled.</td>
</tr>
<tr>
<td></td>
<td>Off when the DMZ is disabled.</td>
</tr>
<tr>
<td>VPN</td>
<td>Off when no VPN tunnel is defined, or all defined VPN tunnels have been disabled.</td>
</tr>
<tr>
<td></td>
<td>Solid green when at least one VPN tunnel is up.</td>
</tr>
<tr>
<td></td>
<td>Flashing green when sending or receiving data over VPN tunnel.</td>
</tr>
<tr>
<td></td>
<td>Solid amber when no enabled VPN tunnel is up.</td>
</tr>
<tr>
<td>USB1 and USB2</td>
<td>Off when no USB device is connected, or is inserted but not recognized.</td>
</tr>
<tr>
<td></td>
<td>Solid green when the USB dongle is connected to the ISP successfully. USB storage is recognized.</td>
</tr>
<tr>
<td></td>
<td>Flashing green when sending or receiving data.</td>
</tr>
<tr>
<td></td>
<td>Solid amber when the USB dongle is recognized but fails to connect to ISP (no IP address is assigned). The USB storage access has errors.</td>
</tr>
<tr>
<td>RESET</td>
<td>To reboot the device, press the reset button with a paper clip or pen tip for less than 10 seconds.</td>
</tr>
<tr>
<td></td>
<td>To reset the device to factory default settings, press and hold the reset button for 10 seconds.</td>
</tr>
<tr>
<td>Wireless</td>
<td>LED is on when the internal access point is enabled.</td>
</tr>
<tr>
<td></td>
<td>LED is off when the internal access point is disabled.</td>
</tr>
</tbody>
</table>
### Getting Started

You can use the various links available on this page and follow the on-screen instructions to quickly configure your network device.

#### Launch Setup Wizard

<table>
<thead>
<tr>
<th>Wizard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Setup Wizard</td>
<td>Directs you to the Initial Setup Wizard.</td>
</tr>
<tr>
<td>VPN Setup Wizard</td>
<td>Directs you to the VPN Status Wizard.</td>
</tr>
<tr>
<td>Application Control Wizard</td>
<td>Directs you to the Application Control Wizard.</td>
</tr>
</tbody>
</table>

#### Initial Configuration

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Administrator Password</td>
<td>Directs you to the User Accounts page where you can change the administrator password and set up a guest account.</td>
</tr>
<tr>
<td>Configure WAN Settings</td>
<td>Directs you to the WAN Settings page where you can modify the WAN parameters.</td>
</tr>
<tr>
<td>Configure USB Settings</td>
<td>Directs you to the Mobile Network page where you can modify the USB configurations.</td>
</tr>
<tr>
<td>Configure VLAN Settings</td>
<td>Directs you to the VLAN Membership page where you can configure the VLAN.</td>
</tr>
</tbody>
</table>

#### Quick Access

<table>
<thead>
<tr>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrade Firmware</td>
<td>Directs you to the File Management page where you can update the device firmware.</td>
</tr>
<tr>
<td>Configure Remote Management Access</td>
<td>Directs you to the FireWall &gt;Basic Settings page where you can enable the basic features of the device.</td>
</tr>
<tr>
<td>Backup Device Configuration</td>
<td>Directs you to the Config Management page where you can manage the device’s configuration.</td>
</tr>
</tbody>
</table>

#### Device Status

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Summary</td>
<td>Directs you to the System Summary page that displays the IPv4 and IPv6 configuration, and firewall status on the device.</td>
</tr>
<tr>
<td>VPN Status</td>
<td>Directs you to the VPN Status page that displays the status of the VPNs managed by this device.</td>
</tr>
<tr>
<td>Port Statistics</td>
<td>Directs you to the Port Traffic page which displays the device’s port status and port traffic.</td>
</tr>
<tr>
<td>Traffic Statistics</td>
<td>Directs you to the TCP/IP Services page which displays the device’s port listen status and the established connection status.</td>
</tr>
<tr>
<td>View System Log</td>
<td>Directs you to the View Logs page which displays the logs on the device.</td>
</tr>
</tbody>
</table>
Troubleshooting Tips

If you have trouble connecting to the Internet or the web-based web interface:

• Verify that your web browser is not set to work offline.

• Check the local area network connection settings for your Ethernet adapter. The PC should obtain an IP address through DHCP. Alternatively, the PC can have a static IP address in the 192.168.1.x range with the default gateway set to 192.168.1.1 (the default IP address of the device).

• Verify that you entered the correct settings in the Wizard to set up your Internet connection.

• Reset the modem and the device by powering off both devices. Next, power on the modem and let it sit for about 2 minutes. Then, power on the device. You should now receive a WAN IP address.

• If you have a DSL modem, ask your ISP to put the DSL modem into bridge mode.

User Interface

The user interface is designed to make it easy for you to set up and manage your device.

Navigation

The major modules of the web interface are represented by buttons in the left navigation pane. Click a button to view more options. Click an option to open a page.

Popup windows

Some links and buttons launch popup windows that display more information or related configuration pages. If your web browser displays a warning message about the popup window, allow the blocked content.

Help

To view information about the selected configuration page, click Help at the top right corner of the web interface. If your web browser displays a warning message about the popup window, allow the blocked content.

Logout

To exit the web interface, click Logout near the top right corner of the web interface. The sign-in page appears.

The user interface is designed to make it easy to set up and manage the device. The header toolbar icons are described in the table below.

Table 2: Header Toolbar Options

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Toggle button</strong> – Located on the top left of the header – This toggle button helps to expand or collapse the navigation pane.</td>
</tr>
<tr>
<td></td>
<td><strong>Language Selection</strong> – This drop-down list allows you to select the language for the user interface.</td>
</tr>
</tbody>
</table>
## User Interface

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Help" /></td>
<td>Help – The online-help documentation for the device.</td>
</tr>
<tr>
<td><img src="image" alt="About" /></td>
<td>About – The firmware version information for the device.</td>
</tr>
<tr>
<td><img src="image" alt="Logout" /></td>
<td>Logout – Click to log out of the device.</td>
</tr>
</tbody>
</table>

### Icon Legend

This table displays the most common icons found throughout the graphical interface and their meanings.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Add" /></td>
<td>Add – Click to add an entry.</td>
</tr>
<tr>
<td><img src="image" alt="Edit" /></td>
<td>Edit – Click to edit an entry.</td>
</tr>
<tr>
<td><img src="image" alt="Delete" /></td>
<td>Delete – Click to delete an entry.</td>
</tr>
<tr>
<td><img src="image" alt="Refresh" /></td>
<td>Refresh – Click to refresh the data.</td>
</tr>
<tr>
<td><img src="image" alt="Reset counters" /></td>
<td>Reset counters – Click to reset the counters.</td>
</tr>
<tr>
<td><img src="image" alt="Clone" /></td>
<td>Clone – Click to clone the settings.</td>
</tr>
<tr>
<td><img src="image" alt="Export" /></td>
<td>Export – Click to export the configurations.</td>
</tr>
<tr>
<td><img src="image" alt="Import" /></td>
<td>Import – Click to import the configurations.</td>
</tr>
<tr>
<td><img src="image" alt="Save" /></td>
<td>Save – Click to save the configurations.</td>
</tr>
</tbody>
</table>
Connected – Click to connect.

Disconnected – Click to disconnect.

Popup Windows

Some links and buttons launch popup windows that display more information or related configuration pages. If the web browser displays a warning message about the popup window, allow the blocked content.
Status and Statistics

This section provides information on the various configuration settings of your device and contains the following topics:

- System Summary, on page 7
- TCP/IP Services, on page 9
- Port Traffic, on page 10
- WAN QoS Statistics, on page 11
- ARP Table, on page 11
- Routing Table, on page 12
- DHCP Bindings, on page 12
- Mobile Network, on page 13
- View Logs, on page 13
- Captive Portal Status, on page 14

System Summary

The System Summary provides a snapshot of the settings on your device. It displays your device’s firmware, serial number, port traffic, routing status, mobile networks, and VPN server settings. To view this System Summary, click Status and Statistics > System Summary.

System Information

- **Host Name** – Name of host.
- **Serial Number** – Serial number of the device.
- **System Up Time** – Length of time in yy-mm-dd, hours, and minutes that the device has been active.
- **Current Time** – Current time and date.
- **PID VID** – Version number of the hardware.

Firmware Information

- **Firmware Version** – Version number of the installed firmware.
- **Firmware MD5 Checksum** – A value used for file validation.
• **WAN1 MAC Address** – The MAC address of WAN1.
• **WAN2 MAC Address** – The MAC address of WAN2.
• **LAN MAC Address** – The MAC address of the LAN.

**Port Status**
• **Port ID** – Defined name and number of the port.
• **Interface** – Name of the port used for the connection.
• **Link Status** – Status of the link.
• **Speed** – The speed (in Mbps) of the device after auto negotiation.

**Radio Status**
Radio 1 (2.4GHz) and Radio 2 (5GHz)
• **Wireless Radio** – Displays if the wireless radio is enabled or disabled.
• **MAC Address** – MAC address for the wireless connection.
• **Mode** - Supported wireless network (802.11b/g/n for 2.4 GHz radio) and (802.11a/n/ac for 5 GHz radio).
• **Channel** - Bandwidth channel for wireless connection. (Channel 11 for 2.4GHz radio and channel 42 for 5 GHz radio).
• **Operational Bandwidth**
  - Operational bandwidth for the wireless radio (20/40MHZ for 2.4GHz and 80MHz for 5 GHz)

**IPv4 and IPv6**
• **Interface** – Name of the interface.
• **IP Address** – IP address assigned to the interface.
• **Default Gateway** – Default gateway for the interface.
• **DNS** – IP address of the DNS server.
• **Dynamic DNS** – IP address of the DDNS for the interface: Disabled or Enabled.
• **Multi-WAN Status** - Displays the multi-WAN status: Offline or Online.
• **Renew** – Click to renew the IP address.

**VPN Status**
• **Type** – Type of the VPN tunnel.
• **Enabled** – Is Enabled or Disabled.
• **Configured** – VPN tunnel’s status whether it is configured or not.
• **Max Supported Sessions** – The maximum number of tunnels supported on the device.
• **Connected Sessions** – Current status of the tunnel.

**Firewall Setting Status**

• **Stateful Packet Inspection (SPI)** – also known as dynamic packet filtering, monitors the state of active connections and uses this information to determine which network packets are allowed through the firewall.

• **Denial of Service (Dos)** – Status of the Dos filter service is enabled (On) or disabled (Off). A DoS attack is an attempt to make a machine or network resource unavailable to its intended users.

• **Block WAN Request** – Makes it difficult for outside users to work their way into your network by hiding the network ports from Internet devices and preventing the network from being detected by other Internet users.

• **Remote Management** – Indicates that a remote connection for managing the device is allowed or denied.

• **Access Rule** – Number of access rules that have been set.

**Log Setting Status**

• **Syslog Server** – Status of system logs.

• **Email Log** – Status of logs to send using email.

**TCP/IP Services**

The TCP/IP Services page displays the status of the protocol, port, and IP address. To view the TCP/IP services, click **Status and Statistics > TCP/IP Services**.

**Port Listen Status**

• **Protocol** – Type of protocol used for communication.

• **Listen IP Address** – The listening IP address on the device.

• **Listen Port** – The listening port on the device.

**Established Connection Status**

• **Protocol** – Type of protocol used for communication.

• **Local IP Address** – IP address of the system.

• **Local Port** – Listening ports on different services.

• **Foreign Address** – IP address of the device connected.

• **Foreign Port** – Port of the device connected.

• **Status** – Connection status of the session.
Port Traffic

The Port Traffic page displays the status of the interfaces of the device. To view the device’s Port Traffic page, click Status and Statistics >Port Traffic.

Port Traffic

- **Port ID** – Defined name and number of the port.
- **Port Label** – Name of the port.
- **Link Status** – Status of the link.
- **Rx Packets** – Number of packets received on the port.
- **Rx Bytes** – Number of packets received, measured in bytes.
- **Tx Packets** – Number of packets transmitted on the port.
- **Tx Bytes** – Number of packets transmitted and measured in bytes.
- **Packet Error** – Number of packets not successfully received on the device.

Wireless Traffic (RV340W)

- **SSID Name** – Name of the SSID.
- **VLAN** – VLAN ID.
- **Radio Name** – Name of wireless radio.
- **Status** – Wireless status.
- **Rx Packets** – Number of packets received on the port.
- **Rx Bytes** – Number of packets received, measured in bytes.
- **Tx Packets** – Number of packets transmitted on the port.
- **Tx Bytes** – Number of packets transmitted and measured in bytes.
- **Multicast Packets** – Number of multicast packets transferred on the device.
- **Packet Error** – Number of packets not successfully received on the device.
- **Packet Dropped** – Number of packets dropped by the device.
- **Collisions** – Number of packets colluded on the device.
- **No of clients** – Number of clients (devices) connected to the wireless.

Port Status

- **Port ID** – Defined name and number of the port.
- **Port Label** – Name of the port.
• **Link Status** – Status of the interface.
• **Port Activity** – Status of the port (example: port enabled or disabled or connected).
• **Speed Status** – The speed (in Mbps) of the device after auto negotiation.
• **Duplex Status** – Duplex mode: Half or Full.
• **Auto Negotiation** – Status of the auto negotiation parameter. When enabled (**On**), it detects the duplex mode, and if the connection requires a crossover, automatically chooses the MDI or MDIX configuration that matches the other end of the link.

**WAN QoS Statistics**

The WAN QoS Statistics page displays the statistics of the outbound and inbound WAN QoS. To view the device’s WAN QoS Statistics page, click **Status and Statistics > WAN QoS Statistics**.

- **Interface** – Name of the interface.
- **Policy Name** – Name of the policy.
- **Description** – Description of the WAN QoS statistics.
- **Counters last reset** – Click to reset the counters.

**Outbound QoS Statistics**

- **Queue** – Number of outbound queues.
- **Traffic Class** – Name of traffic class assigned to queue.
- **Packets Sent** – Number of outbound packets of the traffic class sent.
- **Packets Dropped** – Number of outbound packets dropped.

**Inbound QoS Statistics**

- **Queue** – Number of inbound queues.
- **Traffic Class** – Name of traffic class assigned to queue.
- **Packets Sent** – Number of traffic class inbound packets sent.
- **Packets Dropped** – Number of inbound packets dropped.

**ARP Table**

The ARP Table lists all of the devices currently connected and their stats.

To open the Connected Devices page, click **Status and Statistics > ARP Table**.

- **Hostname** – Name of the connected device.
- **IPv4** – The IPv4 address of the connected devices.
• MAC Address – MAC address of the connected device.
• Type – Shows the type of the device IP address.
• Interface – Displays the connection to which interface it is connected.

IPv6
• IPv6 Address – Displays the IPv6 address of the connected device.
• MAC Address – MAC address of the connected device.

Routing Table
Routing is the process of moving packets across a network from one host to another. The routing table contains information about the topology of the network immediately around it. To view the IPv4 and IPv6 routes, click Status and Statistics > Routing Table.

IPv4 and IPv6 Routes
• Destination – IP Address and subnet mask of the connection.
• Next Hop – IP address of the next hop. Maximum number of hops (the maximum is 15 hops) that a packet passes through.
• Metric – Number of routing algorithms when determining the optimal route for sending network traffic.
• Interface – Name of the interface to which the route is attached to.
• Source – Source of the route (Connected, Dynamic).

DHCP Bindings
The DHCP Bindings table displays the status of the DHCP client information such as IPv4/IPv6 address, MAC address, lease expires time and type of binding (static or dynamic). To view the device’s DHCP bindings, click Status and Statistics > DHCP Bindings.

In the DHCP Bindings Table, the following is displayed:
• IPv4 Address/IPv6 Address – Assigned IP address to the clients.
• MAC Address – The MAC address of the clients’ assigned IP address.
• Lease Expires – Lease time for the client’s system.
• Type – Shows the status of the connection (Static or Dynamic).
• Action – Allows you to delete one of the connections from the binding table.
Mobile Network

Mobile networks enables a device and its subnets to be mobile while continuing to maintain IP connectivity transparent to the IP hosts connecting to the network through this mobile device. To view the device’s mobile network, click Status and Statistics > Mobile Network. Next, select the Interfaces from the drop-down list (USB1 or USB2). Click Refresh to refresh mobile network status.

Connection

- **Internet IP Address** – IP address served by the service provider.
- **Subnet Mask** – Mask served by the service provider.
- **Default Gateway** – Default gateway served by the service provider.
- **Connection Up Time** – Time duration of connected device.
- **Current Dial-Up Session Usage** – Data usage per session.
- **Monthly Usage** – Monthly data usage.

Data Card Status

- **Manufacturer** – Manufacturer of the device.
- **Card Firmware** – Firmware version provided by the manufacturer.
- **SIM Status** – Status of the SIM.
- **IMSI** – Unique number of the device.
- **Carrier** – Name or type of data carrier.
- **Service Type** – Data service type.
- **Signal Strength** – Strength of data signal.
- **Card Status** – Card status disconnected or connected.

View Logs

The View Logs page displays all of the device’s logs. You can filter these logs based on category, severity, or keyword. You can also refresh, clear, and export these logs to a PC or USB. To view the device’s logs, follow these steps:

**Step 1**  Click Status and Statistics > View Logs.

**Step 2**  Under Logs Filtered By, select the appropriate option.
Click any of the following to view logs:

- **All** – Displays all the logs.
- **Category** – Displays the selected category logs.

**Severity**
Select one of the options displayed to view the logs based on the severity.

**Search Keyword**
Enter a keyword to display the logs based on the keyword.

---

**Step 3**
Click **Show Logs**.

**Note**
To configure log settings, see Log, on page 26.

**Step 4**
Click any of the following options:

- **Refresh** – Click to refresh logs.
- **Clear Logs** – Click to clear logs.
- **Export Logs to PC** – Click to export logs to PC.
- **Export Logs to USB** – Click to export logs on to a USB storage device.

---

**Captive Portal Status**

Captive portal support enables a highly secure, customized guest access with multiple rights and roles. It provides secure wireless Internet access to visiting customers and rapid authentication and connectivity for employees who are using their personal mobile devices.

To open and see the Captive Portal Status, click **Status and Statistics > Captive Portal Status**.

Select the required SSID from the drop-down to see the following details.

**Step 1**
Select the required SSID from the drop-down to see the following details:

- **Username** — Name of the connected user.
- **SSID** — Name of the network
- **IP Address** — IP address served by the service provider.
- **MAC Address** — Mask served by the service provider.
- **Auth** — Default gateway served by the service provider.
- **Tx Bytes** — Number of packet transmitted and measured in bytes
- **Rx Bytes** — Number of packet received, measured in bytes.
- **Connected Time** — Time duration of connected device.
Step 2 Select the required user and click **Disconnect** to disconnect the device. Then, click **Refresh** to refresh the data on the page.
CHAPTER 3

Administration

This section describes the device's administration features and contains the following topics:

- File Management, on page 17
- Reboot, on page 20
- Diagnostic, on page 20
- Certificate, on page 21
- Configuration Management, on page 22

File Management

The File Management provides a snapshot of your device. To view the File Management info, follow these steps:

**Step 1** Click Administration > File Management, to see the following information:

System Information

- **Device Model** – Model number of the device.
- **PID VID** – PID and VID number of the device.
- **Current Firmware Version** – Current firmware version.
- **Latest Updated** – Date of last firmware update.
- **Last Checked** – Date when last checked.

Signature

- **Current Signature Version** – Version of the signature.
- **Last Update** – Last date of when an update was performed.
- **Last Checked** – Date when last checked.

USB Dongle Driver
Manual Upgrade

In the Manual Upgrade section, you can upload and upgrade to a newer version of the firmware, signature file, USB dongle driver or language file.

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 device unusable.

Step 2 If you select to upgrade from the USB drive, the device will search the USB flash drive for a firmware image file whose name has one or more of the following: PID, MAC address, and Serial Number. If there are multiple firmware files in the USB flash drive, the device will check the one with the most specific name, i.e. priority from high to low.

Auto Update

The device supports loading a firmware from USB flash drive if the USB stick is present during the system bootup. The device will search the USB flash drive for a firmware image file whose name has one or more of the following: PID, MAC address, and Serial Number. If there are multiple firmware files in the USB flash drive, the device will check the one with the most specific name, i.e. priority from high to low.
The files with other names will be ignored. If the version is higher than the current version, it will be upgraded to this image and the DUT will reboot. After that, the upgrade process will start again.

If it does not find a more recent image in the USB1, then it will check the USB2 using the same logic.

The device also supports loading a configuration file from a USB flash drive during the system bootup.

- The behavior only happens when the device is in factory default and attached with a USB flash drive before it is.
- The device will search the USB flash drive for a config file whose name has one or more of the following: PID, MAC address, and Serial Number. If there are multiple firmware files in the USB flash drive, the device will check.
  - the one with the most specific name, i.e. priority from high to low.
    - PID-MAC-SN.xml
    - PID-SN.xml
    - PID-MAC.xml
    - PID.xml

The files with the other names will be ignored.

**Firmware Auto Fallback Mechanism**

The device includes two firmware images in the flash to provide an Auto Fallback Mechanism so that the device can automatically switch to the secondary firmware when the active firmware is corrupted or cannot boot up successfully after five trials.

The Auto Fallback Mechanism operates as follows:

1. The device first boots up with the active firmware.
2. If the firmware is corrupted, it will switch to the secondary firmware automatically after the active firmware has failed to boot up after 5 times. If the device gets stuck does not reboot automatically, you can turn off the power, power on, wait for 30 seconds, then turn off the power, for 5 times to switch to the secondary or inactive firmware.
3. After booting up with the secondary or inactive firmware, please check to see if anything is wrong with the active firmware.
4. Reload the new firmware again if necessary.
Reboot

The Reboot allows users to restart the device with active or inactive images.

To access Reboot page, follow these steps:

**Step 1**  
Click **Administration > Reboot**.

**Step 2**  
In the Active Image after Reboot section, select an option (**Active Image x.x.x.x** or **Inactive Image x.x.x.x**) from the drop-down list.

**Step 3**  
Select the preferred reboot option.

- Reboot the device.
- Return to factory default settings after reboot.
- Return to factory default settings including certificates after reboot.

**Step 4**  
Click **Reboot** to reboot device.

Diagnostic

Your device provides several diagnostic tools to help you with troubleshooting network issues. Use the following diagnostic tools to monitor the overall health of your network.

**Using Ping or Trace**

You can use the Ping or Trace utility to test connectivity between this device and another device on the network. To use Ping or Trace, follow these steps:

**Step 1**  
Select **Administration > Diagnostic**.

**Step 2**  
In the Ping or Trace an IP Address section, in the IP Address/Domain Name field, enter an IP address or domain name.

**Step 3**  
Click **Ping**. The ping results appear. This tells you if the device is accessible. Or click **Traceroute**. The traceroute results appear.

**Step 4**  
To perform a DNS lookup, enter the IP address or domain name in the Perform a DNS Lookup>IP Address/Domain Name field and click **Lookup**.

**Step 5**  
To view and export a technical support report, click one of the following options:

- **Export To PC** - Select this option to export the report to your PC.
- **Export to USB** - Select this option to export the report to a USB device.
- **Email to** - Select this option to email the report to an address.
Certificate

Certificates are important in the communication process. The certificate signed by a trusted Certificate Authority (CA), ensures that the certificate holder is really who he claims to be. Without a trusted signed certificate, data may be encrypted, however, the party you are communicating with may not be the one whom you think.

A list of certificates with the certificate details are displayed on this page. You can export a Self signed, local, and CSR certificate. Or, you can import a CA, Local, or PKCS#12 certificate. You can also import a certificate file (from PC/USB) to a new certificate.

If a device certificate is imported, it replaces its corresponding CSR certificate.

On Certificate Table, the certificates that are associated to the device are displayed. You can delete, export, view the details, or import a certificate that is listed in the Certificate Table.

Import Certificate

To import a certificate, follow these steps:

Step 1  Click Import Certificate.
Step 2  Select the type of certificate to import from the drop-down list:
   - Local Certificate
   - CA Certificate
   - PKCS#12 encoded file.
Step 3  Enter a certificate name. (For PKCS#12, you must enter a password).
Step 4  Check Import from PC and click Choose File to upload and import the certificate from a specific location.
Step 5  Check Import From USB and click Refresh to upload and import the certificate from a USB key.
Step 6  Click Upload.

Generate CSR/Certificate

Step 1  Click Generate CSR/Certificate.
Step 2  Select the type of certificate to generate from the drop-down list.
Step 3  Enter the following information:

<table>
<thead>
<tr>
<th>Certificate Name</th>
<th>Enter a name for certificate. Certificate name should not contain spaces or special characters.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject Alternative Name</td>
<td>Enter a name and select one of the following: IP Address, FQDN, or Email.</td>
</tr>
<tr>
<td>Country Name</td>
<td>Select a country from the drop-down list.</td>
</tr>
<tr>
<td>State or Province Name</td>
<td>Enter a State or Province.</td>
</tr>
<tr>
<td><strong>Locality Name</strong></td>
<td>Enter a locality name.</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td><strong>Organization Name</strong></td>
<td>Enter the name of the organization.</td>
</tr>
<tr>
<td><strong>Organization Unit Name</strong></td>
<td>Enter the name of the organization unit.</td>
</tr>
<tr>
<td><strong>Common Name</strong></td>
<td>Enter a common name.</td>
</tr>
<tr>
<td><strong>Email Address</strong></td>
<td>Enter the email address.</td>
</tr>
<tr>
<td><strong>Key Encryption Length</strong></td>
<td>Select the Key Encryption Length from the drop-down menu. It should be 512, or 2048.</td>
</tr>
<tr>
<td><strong>Valid Duration</strong></td>
<td>Enter the number of days (Range 1-10950, Default: 360).</td>
</tr>
</tbody>
</table>

**Step 4**
Click **Generate**.

---

**Built-In 3rd-Party CA Certificates**

**Step 1**
Click **Show Built-In-3rd Party CA Certificates**.

**Step 2**
Select a certificate from the Certificate Table and click **Export**.

**Step 3**
Choose one of the following options:

- Export as PKCS#12 format - Select this option to export this certificate as PKCS#12 format.
- Export as PEM format - Select this option to export as PEM certificate type.
- Select Destination to Export - Select this option to export to PC or USB.

---

**Select as Primary Certificate**

**Step 1**
Click **Select as Primary Certificate**.

**Step 2**
In the Certificate Table, select the check-box of the appropriate certificate and click **Select as Primary Certificate**.

---

**Configuration Management**

Config Management page provides details on the device’s file configurations.

**Configuration File Name**

The Configuration File Name displays the last changed time details on the following:

- **Running Configuration** - All configurations that the device is currently using are in the Running Configuration file which is volatile and is not retained between reboots.
• **Startup Configuration** - Contains all configurations that were last saved which are loaded into the Running Configuration file after reboot.

• **Mirror Configuration** - The device automatically copies the Startup configuration to the Mirror configuration after 24 hours of running in stable condition (no reboots and no configuration changes within the 24-hour period).

• **Backup Configuration** - It is simply an additional copy of configuration file used as a backup. It remains unchanged until it is being written over.

**Copy/Save Configuration**

The Copy/Save Configuration section displays the default configuration of the device uses the running configuration file, which is unstable and does not retain the settings between reboots. You can save this running configuration file to the startup configuration file.

• **Source** – Select the source file name from the drop-down list.

• **Destination** – Select the destination file name from the drop-down list.

• **Save Icon Blinking** – Indicates whether an icon blinks when there is unsaved data. To disable/enable this feature, click **Enabled Save Icon Blinking** or **Disabled Save Icon Blinking**.
System Configuration

The System Configuration section provides guidance when installing and configuring the device and contains the following topics:

- System, on page 25
- Time, on page 26
- Log, on page 26
- Email, on page 28
- User Accounts, on page 29
- User Groups, on page 32
- IP Address Groups, on page 33
- SNMP, on page 34
- Discovery-Bonjour, on page 35
- LLDP, on page 35
- Automatic Updates, on page 36
- Schedules, on page 36
- Service Management, on page 37
- PnP (Plug and Play), on page 37

System

Your ISP may assign a hostname and a domain name to identify your device or require you to specify the same. In the former case, the default values can be changed as needed. Follow these steps to assign a host and domain name.

**Step 1** Click **System Configuration > System**.
**Step 2** In the Host Name field, enter a host name.
**Step 3** In the Domain Name field, enter a domain name.
**Step 4** Click **Apply**.
Time

Setting the time is critical for a network device so that every system log and error message is timestamped for accurate tracking and synchronizing the data transfer with other network devices.

You can configure the time zone, adjust for daylight savings time if necessary, and select the Network Time Protocol (NTP) server to synchronize the date and time.

To configure the time and NTP server settings, follow these steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Click System Configuration &gt; Time.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Set Time Zone– Select your time zone relative to Greenwich Mean Time (GMT).</td>
</tr>
<tr>
<td>Step 3</td>
<td>Set Date and Time – Select Auto or Manual.</td>
</tr>
<tr>
<td>a)</td>
<td>Auto – Check Default or User Defined for the NTP Server and enter a qualified NTP Server name.</td>
</tr>
<tr>
<td></td>
<td>b) Manual – Enter the date and time.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Set Daylight Savings Time– Check to enable daylight savings time. You can choose the Daylight Saving Mode – By Date or Recurring and enter the start dates and end dates. You can also specify the Daylight Saving Offset in minutes.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Apply.</td>
</tr>
</tbody>
</table>

Log

One of the basic settings of a network device is its system log (Syslog), which is used to log the device data. You can define the instances that should generate a log. Whenever such defined instance occurs, a log is generated with the time and event and sent to a syslog server or sent in an email. Syslog can then be used to analyze and troubleshoot a network and to increase the network security.

Configure Log Settings

To configure the log settings, follow these steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Click System Configuration &gt; Log.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Under Log Setting, in the Log section, check Enable.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Log Buffer field, enter the number of KB (Range 1 KB to 4096 KB, Default is 1024 KB). It is an area in memory where redo is temporarily stored before it can be written to a disk. The acceptable range of the size is 1 to 4096 KB; and the default size is 1024 KB.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Select the appropriate log severity level from the Severity drop down list. They are listed from the highest to the lowest.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Emergency</th>
<th>Level 0, which means that the system is unusable.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert</td>
<td>Level 1, which indicates that immediate action is needed.</td>
</tr>
<tr>
<td>Critical</td>
<td>Level 2, which indicates that the system is in critical condition.</td>
</tr>
<tr>
<td>Error</td>
<td>Level 3, which indicates that there is an error in the device, such as a single port being off-line.</td>
</tr>
</tbody>
</table>
**Warning**
Level 4, which indicates that a warning message is logged when the device is functioning properly, but an operational problem has occurred.

**Notification**
Level 5, which indicates a normal but significant condition. A notification log is logged when the device is functioning properly, but a system notice has occurred.

**Information**
Level 6, which indicates a condition that is not a condition error, but requires special handling.

**Debugging**
Level 7, which indicates that the debugging messages contain information normally of use only when debugging a program.

---

**Step 5**
Check All or any of the required event categories that you want logged on the device.

<table>
<thead>
<tr>
<th>Kernel</th>
<th>Logs involving kernel code.</th>
</tr>
</thead>
<tbody>
<tr>
<td>License</td>
<td>Logs involving license violations.</td>
</tr>
<tr>
<td>System</td>
<td>Logs related to user-space applications such as NTP, Session, and DHCP.</td>
</tr>
<tr>
<td>Web Filter</td>
<td>Logs related to events that triggered web filtering.</td>
</tr>
<tr>
<td>Firewall</td>
<td>Logs related to firewall rules, attacks, and content filtering.</td>
</tr>
<tr>
<td>Application Control</td>
<td>Logs related to application control.</td>
</tr>
<tr>
<td>Network</td>
<td>Logs related to routing, DHCP, WAN, LAN, and QoS.</td>
</tr>
<tr>
<td>Users</td>
<td>Logs related to users activities.</td>
</tr>
<tr>
<td>VPN</td>
<td>VPN-related logs including instances like VPN tunnel establishment failure, VPN gateway failure, and so on.</td>
</tr>
<tr>
<td>3G/4G</td>
<td>Logs from the 3G/4G dongles which are plugged into the device.</td>
</tr>
<tr>
<td>SSLVPN</td>
<td>Logs related to SSLVPN.</td>
</tr>
<tr>
<td>PnP</td>
<td>Logs related to Cisco's Plug-n-Play.</td>
</tr>
</tbody>
</table>

**Step 6**
To save the logs to a USB drive, check **Save to USB Automatically**, and select the USB to save the logs.

---

**Email Server**

The email server can be configured to your email account. The email server logs are periodically sent to specific email address, so that the administrator is always up to date on the network. The device supports SMTP mail account configuration such as email addresses, password, message digest; optional parameters, SMTP server port number, SSL, TLS.

**Step 1**
In the **Email Server** section, check **Email Syslogs** to enable the device to send email alerts when events are logged.

**Step 2**
In the **Email Settings** section, click **Link to Email Setting** page to configure your email settings.

**Step 3**
In the **Email Subject** section, enter the subject.

**Step 4**
In the **Severity** section, select the severity level from the drop-down list.

**Step 5**
In the **Log Queue Length** section, enter a range from 1 to 1000. The default is 50.

**Step 6**
In the **Log Time Threshold** section, select the time threshold from the drop-down list.
**Remote Syslog Server**

A remote syslog server allows you to separate the software that generates the messages and events from the system that stores and analyzes them. When enabled, the network driver sends messages to a syslog server on the local Intranet or Internet through a VPN tunnel. The syslog server can be configured by specifying the name or IP address.

**Step 1**
In the **Syslog Server** section, check **Enable** to enable sending system logs to a remote server.

**Step 2**
In the Syslog Server fields, enter the information below:

<table>
<thead>
<tr>
<th>Syslog Server 1</th>
<th>Enter the IP address of the Syslog server to which the log messages should be sent in addition to the local destination.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport</td>
<td>Select UDP or TCP.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port value of the Syslog server.</td>
</tr>
<tr>
<td>Syslog Server 2</td>
<td>Enter the IP address of the Syslog server to which the log messages should be sent in addition to the local destination.</td>
</tr>
<tr>
<td>Transport</td>
<td>Select UDP or TCP.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port value of the Syslog server.</td>
</tr>
</tbody>
</table>

**Step 3**
Click **Apply**.

---

**Email**

You can configure your device’s email server to your specifications.

**Configuring Email**

To configure the email server, follow these steps.

**Step 1**
Select **System Configuration > Email**.

**Step 2**
Under **Email Server**, enter the following:

<table>
<thead>
<tr>
<th>SMTP Server</th>
<th>Enter the address of the SMTP server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP Port</td>
<td>Enter the SMTP port.</td>
</tr>
<tr>
<td>Email Encryption</td>
<td>Select <strong>None</strong> or <strong>TLS/SSL</strong> as the email encryption method.</td>
</tr>
</tbody>
</table>
Select the type of authentication from the drop-down list: None, Login, Plaintext or MD5.

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Select the type of authentication from the drop-down list: None, Login, Plaintext or MD5.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send Email to 1</td>
<td>Enter an email address to send to.</td>
</tr>
<tr>
<td>Send Email to 2</td>
<td>Enter an email address to send to (optional).</td>
</tr>
<tr>
<td>From Email Address</td>
<td>Enter an email address to send from.</td>
</tr>
</tbody>
</table>

**Step 3** Click **Apply and Test Connectivity to Email Server** to test connectivity. Click **Clear** if you which to clear the settings.

**Step 4** Click **Apply**.

---

## User Accounts

You can create, edit, and delete local users and authenticate them using local database for various services like PPTP, VPN Client, Web GUI login, and SSLVPN. This enables the administrators to control and allow only the local users access the network.

To create local users and determine the password complexity, follow these steps:

**Step 1** Select **System Configuration > User Accounts**.

**Step 2** Under Web Login Session Timeout, enter the following information.

<table>
<thead>
<tr>
<th>Administrator Inactivity Timeout</th>
<th>Enter the required admin's inactivity timeout value. By default, 30 mins.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guest Inactivity Timeout</td>
<td>Enter the required guest's inactivity timeout value. By default, 30 mins.</td>
</tr>
</tbody>
</table>

**Step 3** Under **Local Users Password Complexity**, check **Enable** to enable the password complexity.

**Step 4** Configure the password complexity settings.

<table>
<thead>
<tr>
<th>Minimal password length</th>
<th>Enter the minimum length of the password to create a new password (Range 0 to 64, Default 8).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimal number of character classes</td>
<td>Enter the minimum number of character classes that should be used for the new password (Range 0 to 4, Default 3). Compose a password using three of these four classes: (Uppercase, letters, lower case letters, numbers or special characters).</td>
</tr>
<tr>
<td>The new password must be different than the current one</td>
<td>Enable to require the user to enter a different password when the current password expires.</td>
</tr>
<tr>
<td>Password Aging Time</td>
<td>Enter number of days for password expiry. (Range: 0 - 365, 0 means never expire).</td>
</tr>
</tbody>
</table>

**Step 5** In the Local User Membership List section, click **Add** to add a user and enter the following information:

<table>
<thead>
<tr>
<th>Username</th>
<th>Enter a username.</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Password</td>
<td>Enter a password.</td>
</tr>
</tbody>
</table>
Confirm the password.

Select a group (admin or guest) from the drop-down list.

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Click Apply.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 7</td>
<td>Click <strong>Import</strong> to import User Accounts. You can also download the user template using the Download button.</td>
</tr>
<tr>
<td>Step 8</td>
<td>To enable external user authentication using RADIUS, LDAP, and AD use the Remote Authentication Service. Under the Remote Authentication Service Table, click <strong>Add</strong> and enter the following information:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Specify a name for the domain.</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Password</td>
<td>Enter the desired password to use for the user account.</td>
</tr>
<tr>
<td><strong>Authentication Type</strong></td>
<td>Select an authentication type: RADIUS (Remote AuthenticationDial-In User Service), Active Directory (AD), or LDAP.</td>
</tr>
<tr>
<td><strong>Primary Server</strong></td>
<td>Enter the primary IP address of the RADIUS/Active Directory/LDAP server.</td>
</tr>
<tr>
<td><strong>Backup Server</strong></td>
<td>If you have selected RADIUS as the Authentication Type, enter the backup IP address of the server.</td>
</tr>
<tr>
<td><strong>User Container Path</strong></td>
<td>If you have selected Active Directory as the Authentication Type, enter the full path information of the user container. This is where the user login information is available for authenticating the same.</td>
</tr>
<tr>
<td><strong>Base DN</strong></td>
<td>If you have selected LDAP as the Authentication Type, enter the base distinguished name (DN) of the LDAP server. The base DN is the location where the LDAP server searches for users when it receives an authorization request. This field should match the base DN that is configured on the LDAP server.</td>
</tr>
<tr>
<td><strong>Preshared Key</strong></td>
<td>If you have selected RADIUS as the Authentication Type, enter the preshared key of the RADIUS server.</td>
</tr>
<tr>
<td><strong>Confirm Preshared Key</strong></td>
<td>Reenter the preshared key of the RADIUS server to confirm it.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 9</th>
<th>Click Apply.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 10</td>
<td>To enable the service authentication sequences enter the following information:</td>
</tr>
</tbody>
</table>
You can customize the configuration of below services:

- Web Login
- Site-to-site/Ez VPN and 3rd-Party Client-to-site VPN
- AnyConnect SSL VPN
- PPTP Server
- L2TP Server
- 802.1x

**Note** For PPTP Server, L2TP Server, and 802.1x only Local DB and RADIUS authentication types are supported.

**Use Default**

You can toggle based on configuration of the service need. By default, for Web Login, Site-to-site/Ez VPN and 3rd-Party Client-to-site VPN, and AnyConnect SSL VPN services Use Default is selected.

**Note** If this option is enabled the Customize Primary and Customize Secondary options will disabled.

**Customize: Primary**

You can select the required primary authentication type: None, Local DB, RADIUS (Remote Authentication Dial-In User Service), LDAP, or Active Directory.

**Customize: Secondary**

You can select the required secondary authentication type: None, Local DB, RADIUS (Remote Authentication Dial-In User Service), LDAP, or Active Directory.

---

**Remote Authentication Service**

To enable external user authentication using RADIUS and LDAP, use the Remote Authentication Service.

**Step 1**

Under the **Remote Authentication Service Table**, click **Add** and enter the following information:

<table>
<thead>
<tr>
<th>Name</th>
<th>Specify a name for the domain.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authentication Type</strong></td>
<td>Select an authentication type from the drop-down list:</td>
</tr>
<tr>
<td></td>
<td>• <strong>RADIUS</strong> – a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users who connect and use a network service.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Active Directory</strong> – a Windows OS directory service that facilitates working with interconnected, complex and different network resources in a unified manner.</td>
</tr>
</tbody>
</table>
Enter the IP address of the primary server.
**Port** – Enter the primary port of the server.

<table>
<thead>
<tr>
<th>Primary Server</th>
<th>Enter the IP address of the primary server.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Port</strong> – Enter the primary port of the server.</td>
</tr>
</tbody>
</table>

Enter the IP address of the backup server.
**Port** – Enter the backup port of the server.

<table>
<thead>
<tr>
<th>Backup Server</th>
<th>Enter the IP address of the backup server.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Port</strong> – Enter the backup port of the server.</td>
</tr>
</tbody>
</table>

If you have selected RADIUS as the Authentication Type, enter the preshared key of the RADIUS server.

<table>
<thead>
<tr>
<th>Preshared-Key</th>
<th>If you have selected RADIUS as the Authentication Type, enter the preshared key of the RADIUS server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confirm Preshared-Key</td>
<td>Reenter the preshared key of the RADIUS server to confirm it.</td>
</tr>
</tbody>
</table>

### Step 2
Click **Apply** to save the settings. Click **Edit** or **Delete** to edit or delete an existing domain.

**Note**
The external database priority is always RADIUS/LDAP/AD/Local. If you add the Radius server on the device, the Web Login Service and other services will use the RADIUS external database to authenticate the user. There is no option to enable an external database for Web Login Service alone and configure another database for another service. Once RADIUS is created and enabled on the device, the device will use the RADIUS service as an external database for Web Login, Site to Site VPN, EzVPN/3rd Party VPN, SSL VPN, PPTP/L2TP VPN, 802.1x.

---

### User Groups

The administrator can create user groups for a collection of users that share the same set of services. Such user groups can be authorized to access multiple services like Web Login, PPTP, L2TP, and EzVPN.

To create user groups, follow these steps:

#### Step 1
Select **System Configuration > User Groups**.

#### Step 2
Under the User Groups Table, click **Add** to create a new user group.

#### Step 3
In the Group Name field, enter a name for the group.

#### Step 4
Under the Local User Membership List, check the desired check boxes in the Join column to attach the list of users to the group.

#### Step 5
Under Services, select the services the user groups should have access to and enter the following information.

<table>
<thead>
<tr>
<th>Web Login/NETCONF/RESTCONF</th>
<th>Specify the web login permissions granted to the users attached to the group:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Disabled</strong> – No member of the user group can login to the Configuration Utility using a web browser.</td>
</tr>
<tr>
<td></td>
<td><strong>Read Only</strong> – The members of the user group can only read the system status after they login. They cannot edit any settings.</td>
</tr>
<tr>
<td></td>
<td><strong>Administrator</strong> – All members of the user group have full privileges to configure and read the system status.</td>
</tr>
</tbody>
</table>
Site to Site VPN
Check **Permit in this group** to enable access to a site-to-site VPN policy.

- Click **Add** to open the **Add Feature List** pop up.
- Select a profile from the drop down list and click **Add**.

EzVPN/3rd Party
Check **Permit in this group** to enable access to a site-to-site VPN policy.

- Click **Add** to open the **Add Feature List** pop up.
- Select a profile from the drop down list and click **Add**.

SSL VPN
To enable access to a particular policy for the group, select a profile from the Select a Profile drop down list.

PPTP VPN
Check **Permit** to enable PPTP authentication.

L2TP
Check **Permit** to enable L2TP authentication.

802.1x
Check **Permit** to enable 802.1x authentication.

Captive Portal
Check the Permit in this group check box to enable captive portal authentication for the group. Click **Add** to open the Add Feature List pop up. Select a profile from the drop down list and click **Add**.

---

**IP Address Groups**

In order to configure and manage the application control policies and web filtering, you must set up the IP address groups. To configure the IP address groups, follow these steps:

**Step 1**
Click **System Configuration > IP Address Groups**.

**Step 2**
In the **IP Address Group Table**, click **Add** to add a group and enter a name. To delete a group click **Delete**.

**Step 3**
Click **Add** and enter the following information.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Select either IPv4 or IPv6 from the drop down list.</td>
</tr>
<tr>
<td></td>
<td>Select the type of group from the drop-down list, and enter the address details:</td>
</tr>
<tr>
<td></td>
<td>• <strong>IP Address</strong> – Enter an IP address in the IP Address field.</td>
</tr>
<tr>
<td></td>
<td>• <strong>IP Address Subnet</strong> – Enter an IP address in the IP Address filed and its subnet mask in the Mask field.</td>
</tr>
<tr>
<td></td>
<td>• <strong>IP Address Range</strong> – Enter the Start IP Address and End IP Address.</td>
</tr>
</tbody>
</table>

| Address Details | Enter the MAC address of the device to add to this IP group. |
| Device Type     | Select the type of device from the drop-down list. |
SNMP

Simple Network Management Protocol (SNMP) is an Internet-standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior.

Simple Network Management Protocol (SNMP) allows network administrators to manage, monitor, and receive notifications of critical events as they occur on the network. The device supports v1, v2c, and v3 versions. The device acts as an SNMP agent that replies to SNMP commands from SNMP Network Management Systems. The commands it supports are the standard SNMP commands get/next/set. It also generates trap messages to notify the SNMP manager when alarm conditions occur. Examples include reboots, power cycles, and WAN link events.

Step 1
To configure SNMP for your device, enter the following information:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Enable</td>
<td>Check to enable SNMP.</td>
</tr>
<tr>
<td>Allow user access from Internet</td>
<td>Check to allow user from the Internet.</td>
</tr>
<tr>
<td>Allow user access from VPN</td>
<td>Check to allow user access from VPN.</td>
</tr>
<tr>
<td>Version</td>
<td>Select the version from the drop-down list.</td>
</tr>
<tr>
<td>System Name</td>
<td>Enter a system name.</td>
</tr>
<tr>
<td>System Contact</td>
<td>Enter a system contact.</td>
</tr>
<tr>
<td>System Location</td>
<td>Enter a system location.</td>
</tr>
<tr>
<td>Get Community</td>
<td>Enter a name for the community.</td>
</tr>
<tr>
<td>Set Community</td>
<td>Enter a name for the community.</td>
</tr>
</tbody>
</table>

Step 2
In the Trap Configuration section, enter the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trap Receiver IP Address</td>
<td>Enter the IP address.</td>
</tr>
<tr>
<td>Trap Receiver Port</td>
<td>Enter the port number.</td>
</tr>
</tbody>
</table>

Step 4
To add a device, click Add and configure the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>Enter the MAC address of the device to add to this IP group.</td>
</tr>
<tr>
<td>Device and OS Type</td>
<td>Select the appropriate device type and OS from the drop-down list.</td>
</tr>
</tbody>
</table>

Step 5
Click Apply.
Step 3 Click Apply.

Discovery-Bonjour

Bonjour is a service discovery protocol that locates network devices such as computers and servers on your LAN. When this feature is enabled, the device periodically multicasts Bonjour service records to the LAN to advertise its existence.

Note

For discovery of Cisco Small Business products, Cisco provides a utility that works through a simple toolbar on the web browser called FindIt. This utility discovers Cisco devices in the network and displays basic information, such as serial numbers and IP addresses. For more information and to download the utility, visit www.cisco.com/go/findit.

To enable Discovery-Bonjour, follow these steps:

Step 1 Select System Configuration > Discovery-Bonjour.
Step 2 Check Enable, to enable Discovery-Bonjour globally. (It is enabled by default).
Step 3 Check Apply.

LLDP

The Link Layer Discovery Protocol (LLDP) is a vendor-neutral protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on an IEEE 802 local area network. The LLDP information is sent by the device’s interface at a fixed interval, in the form of an Ethernet frame. Each frame contains one LLDP Data Unit (LLDPDU). Each LLDPDU is a sequence of type-length-value (TLV) structure.

To configure LLDP, follow these steps:

Step 1 Select System Configuration > LLDP.
Step 2 In the LLDP section, check Enable. (It is enabled by default).
Step 3 In the LLDP Port Setting Table, check Enable LLDP to enable LLDP on an interface.
Step 4 Click Apply.
Step 5 In the LLDP Neighbors Setting Table, the following information is displayed:
  • Local Port – Port identifier.
  • Chassis ID Subtype – Type of chassis ID (for example, MAC address).
  • Chassis ID – Identifier of the chassis. Where the chassis ID subtype is a MAC address, the MAC address of the device is displayed.
• **Port ID Subtype** – Type of the port identifier.
• **Port ID** – Port identifier.
• **System Name** – Name of the device.
• **Time to Live** – Rate in seconds at which LLDP advertisement updates are sent.

**Step 6** To view details about an LLDP port, select the Local Port and click **Detail**.

**Step 7** To refresh the LLDP Neighbors Setting Table, click **Refresh**.

---

**Automatic Updates**

Upgrading to the latest firmware can help fix bugs and other intermittent issues on the device. For this purpose, the device can be configured to send you email notifying you of important firmware updates for your device. The information can be configured to be sent at specified intervals and for specific types of network events. Before you can configure these notifications, the email server should be configured.

To configure the Automatic Updates, follow these steps:

**Step 1** Select **System Configuration > Automatic Updates**.

**Step 2** From the **Check Every** drop-down list, choose how often the device should automatically check (Never, Week, or Month) for possible firmware revisions. Click **Check Now** to check immediately.

**Step 3** In the **Notify via** field, check Email to and enter the email address. The notifications are sent to a configured email address. If you haven’t configured an email server, you should click the link in the note given beside the email field and configure the email server.

**Step 4** Under **Automatic Update**, select **Notify** to receive notifications for updates.

**Step 5** Select the time from the drop-down list of when the firmware is automatically updated. You can select to receive notifications and configure the updates for the following:

- System Firmware
- USB Modem Firmware
- Security Signature

**Step 6** Click **Apply**.

---

**Schedules**

The network devices should be protected against intentional attacks and viruses that could compromise confidentiality or result in data corruption or denial of service. Schedules can be created to apply firewall or port forwarding rules on specific days or time of day.

To configure the schedule follow these steps.
**System Configuration**

**Service Management**

The Service Management section displays information on the system configuration. You can add a new entry to the Service Management list or to change an entry. To configure the Service Management follow these steps.

**PnP (Plug and Play)**

Network Plug and Play is a service that works in conjunction with Network Plug and Play enabled devices to allow firmware and configuration to be managed centrally, and to allow zero-touch deployment of new network devices. When installed, a Network Plug and Play enabled device will identify the Network Plug and Play server through one of manual configuration, DHCP, DNS, or the Plug and Play Connect service.

To enable or disable Plug and Play, follow these steps:

---

**Step 1** Select **System Configuration > Schedules**.

**Step 2** In the **Schedule Table**, click **Add** to create a new schedule. You can edit an existing schedule by selecting it and clicking **Edit**.

**Step 3** Enter a name to identify the schedule in the **Name** column.

**Step 4** Enter the desired **Start Time** and **End Time** for the schedule.

**Step 5** Check **Everyday** to apply the schedule to all the days of the week. Leave it unchecked if you want it to only apply to certain days. If so, then check the desired days of the week you want to apply the schedule to. You can also choose **Weekday** or **Weekend**.

**Step 6** Click **Apply**.

**Step 1** Click **System Configuration > Service Management**.

**Step 2** In the Service Table, click **Add**.

**Step 3** In the **Application Name** field, enter a 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: (**All**, **TCP & UDP**, **TCP**, **UDP**, **IP**, **ICMP**).

**Step 5** In the **Port Start/ICMP Type/IP Protocol**, enter the port number, ICMP type, or IP protocol.

**Step 6** In the **Port End** field, enter port number.

**Step 7** Click **Apply**.

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

**Step 1** Click **System Configuration > PnP**.

**Step 2** Under **PnP**, check **Enable**.

**Step 3** In the **PnP Transport** field, select an option from the drop-down list.
• **Auto** – PnP Server Discovery downloaded by PnP automatically.

• **Static** – Select and enter IP/FQDN, port number and select the certificate to be imported from the CA Certificate drop-down list.

**Step 4**  Click **Apply**.

**Note**  Please note that the router will verify that the identity configured in the server certificate matches the FQDN or IP address that the router acquires from the DHCP, DNS or the configuration. If the FQDN or IP address is not recognized, the router will refuse to connect to the server. For the Network Plug and Play to work correctly, you should ensure that the certificate lists all variations of the server name and IP address(es) in the Subject Alternative Name field. If you are experiencing issues with your certificate while trying to connect to PnP, please see the Certificate,[ on page 21](#) instructions on how to manage your certificates on the device.

---

### Plug and Play Connect Service

Plug and Play Connect is a Cisco-provided service that is the last resort used by a Network Plug and Play-enabled device to discover the server. To use Plug and Play Connect for server discovery, you must first create a Controller Profile representing the Manager, and then register each of your devices with the Plug and Play Connect Service.

To access the Plug and Play Connect Service, follow these steps:

**Step 1**  In your web browser, navigate to [https://software.cisco.com](https://software.cisco.com).

**Step 2**  Click the **Log In** button at the top right of the screen. Log in with a cisco.com ID associated with your Cisco Smart Account.

**Step 3**  Select the **Plug and Play Connect** link under the **Network Plug and Play** heading. The main page for the Plug and Play Connect service is displayed.

### Creating a Controller Profile

To create a Controller Profile, follow these steps:

**Step 1**  Open the Plug and Play Connect web page [https://software.cisco.com/#module/pnp](https://software.cisco.com/#module/pnp) in your browser. If necessary, select the correct Virtual Account to use.

**Step 2**  Select the Controller Profiles link, and then click **Add Profile**.

**Step 3**  Select a Controller Type of PNP SERVER from the dropdown list. Then click **Next**.

**Step 4**  Specify a name, and optionally a description for the profile.

**Step 5**  Under the heading for Primary Controller, use the drop-down provided to select whether to specify the server by name or IP address. Fill in the name or addresses of the server in the fields provided.

**Step 6**  Select the protocol to use when communicating with the server. It is strongly recommended that HTTPS be used to ensure the integrity of the provisioning process.
Registering Devices

Certain products purchased directly from Cisco may be associated with your Cisco Smart Account at the time of purchase, and these will automatically be added to Plug and Play Connect. However, the majority of Cisco's 100 to 500 series Plug and Play-enabled products will need to be registered manually. To register the devices with Plug and Play Connect, follow these steps:

**Step 1**
Open the Plug and Play Connect web page https://software.cisco.com/#module/pnp in your browser. If necessary, select the correct Virtual Account to use.

**Step 2**
Select the **Devices** link, and then click **Add Devices**. You may need to be approved to manually add devices to your account. This is a one-time process, and, if it is required, you will be notified by email once approval has been granted.

**Step 3**
Choose whether to add devices manually, or to add multiple devices by uploading details in CSV format. Click the link provided to download a sample CSV file. If you choose to upload a CSV file, click the **Browse** button to select the file. Then click **Next**.

**Step 4**
If you selected to add devices manually, click **Identify Device**. Specify the Serial Number and Product ID for the device to be added. Select a Controller Profile from the drop-down. Optionally enter a description for this device.

**Step 5**
Repeat Step 4 until you have added all your devices, then click **Next**.

**Step 6**
Review the devices that you have added, and then click **Submit**.
WAN

This section covers the wide area network (WAN) and contains the following topics:

- WAN Settings, on page 41
- Multi-WAN, on page 44
- Mobile Network, on page 45
- Dynamic DNS, on page 47
- Hardware DMZ, on page 47
- IPv6 Transition, on page 48

WAN Settings

A wide area network (WAN) is a collection of geographically distributed telecommunication or computer network. The term distinguishes a broader telecommunication structure from a local area network (LAN). A wide area network may be privately owned or rented and allows a business to effectively carry out its daily functions regardless of its location.

There are two physical WAN and VLAN interfaces which can be configured on the device. To configure the WAN settings, follow these steps

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Select <strong>WAN &gt; WAN Settings</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the WAN table, click <strong>Add or Edit</strong> and configure the settings for the IPv4, IPv6, or Advanced.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select the sub-interface name and enter the VLAN ID.</td>
</tr>
</tbody>
</table>

**IPv4 and IPv6 Connections**

<table>
<thead>
<tr>
<th>Step 4</th>
<th>For an IPv4 connection, click the <strong>IPv4</strong> tab.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5</td>
<td>Select the connection type from the list:</td>
</tr>
</tbody>
</table>

**When the IPv4 or IPv6 connection uses DHCP**

In the DHCP settings, enter the following information:

<table>
<thead>
<tr>
<th>Static DNS 1 &amp; 2</th>
<th>Enter the IP address of the primary and or secondary Static DNS in the fields.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DHCP-PD</strong> (IPv6 only)</td>
<td>Check to enable and enter a prefix name.</td>
</tr>
</tbody>
</table>

**When the IPv4 or IPv6 connection uses Static IP**

In the **Static IP Settings**, enter the following information:
### WAN Settings

<table>
<thead>
<tr>
<th><strong>IP Address</strong></th>
<th>Enter the IP address.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Netmask</strong></td>
<td>Enter the netmask.</td>
</tr>
<tr>
<td><strong>Default Gateway</strong></td>
<td>Enter the IP address of the default gateway. Default Gateway is needed on this interface to participate in the load balance and failover (Multi-WAN).</td>
</tr>
<tr>
<td><strong>DNS Server</strong></td>
<td>Select Use DNS as Below.</td>
</tr>
<tr>
<td><strong>Static DNS 1 &amp; 2</strong></td>
<td>Enter the IP address of the primary and or secondary Static DNS in the fields.</td>
</tr>
<tr>
<td><strong>DHCP-PD (IPv6 only)</strong></td>
<td>Check to enable and enter a prefix name.</td>
</tr>
</tbody>
</table>

**When the IPv4 or IPv6 connection uses PPPoE**

In the PPPoE Settings section, enter the following information:

| **Share same session with IPv4** | Select Share same session with IPv4 to re-use the same username/password configured in IPv4 PPPoE setting, and obtain IPv4 and IPv6 addresses from the same PPPoE session. |
| **Separate IPv4 and IPv6 sessions** | Select Separate IPv4 and IPv6 sessions for a username/password setting that will be used only for an IPv6 PPPoE session. |
| **Username** | The username assigned to you by the ISP. |
| **Password** | The password assigned to you by the ISP. |
| **DNS Server** | Select Use PPPoE Provided DNS Server or Use DNS as Below. |
| **Static DNS 1 & 2** | Enter the IP address of the primary and or secondary Static DNS in the fields. |
| **Connect Mode** | Select Connect on Demand if your ISP charges when connected. Enter the maximum idle time, in seconds, to wait before terminating the connection due to inactivity. Default is 5 minutes. Select Keep Alive to periodically check the connection, and to re-establish the connection when it is disconnected. |
| **Authentication Type** | Select the authentication type from the drop-down list (Auto, PAP, CHAP, MS-CHAP, MS-CHAPv2). |
| **Service Name** | Enter the name of the service. |
| **DHCP-PD (IPv6 only)** | Check to enable and enter a prefix name. |

**Note** Some service providers do not allow to ping the default gateway, especially for the PPPoE connection. Please go to Multi-WAN page to disable the “Network Service Detection” feature or choose a valid host to detect. Otherwise, the traffic will not be forwarded by the device.

**When the IPv4 connection is through PPTP**

In the PPTP section, enter the following:

<p>| <strong>IP Assignment</strong> | For DHCP, select this option to enable DHCP to provide an IP address. For Static IP, select this option and provide an IP address, netmask, and the IP address of the default gateway. |
| <strong>PPTP Server IP/FQDN</strong> | Enter the name of the server. |
| <strong>Username</strong> | The username assigned to you by the ISP. |
| <strong>Password</strong> | The password assigned to you by the ISP. |</p>
<table>
<thead>
<tr>
<th><strong>DNS Server</strong></th>
<th>Select <strong>Use PPTP Provided DNS Server</strong> or <strong>Use DNS as Below</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Static DNS 1 &amp; 2</strong></td>
<td>Enter the IP address of the primary and or secondary Static DNS in the fields.</td>
</tr>
<tr>
<td><strong>Connect Mode</strong></td>
<td>Select <strong>Connect on Demand</strong> if your ISP charges when connected. Enter the maximum idle time, in seconds, to wait before terminating the connection due to inactivity. Default is 5 minutes. Select <strong>Keep Alive</strong> to periodically check the connection, and to re-establish the connection when it is disconnected.</td>
</tr>
<tr>
<td><strong>Authentication Type</strong></td>
<td>Select the authentication type from the drop-down list (<strong>Auto</strong>, <strong>PAP</strong>, <strong>CHAP</strong>, <strong>MS-CHAP</strong>, <strong>MS-CHAPv2</strong>).</td>
</tr>
<tr>
<td><strong>MPPE Encryption</strong></td>
<td>Check to enable MPPE encryption.</td>
</tr>
</tbody>
</table>

**When the IPv4 connection uses L2TP**

In the L2TP Settings section, enter the following information:

| **IP Assignment**              | For DHCP, select this option to enable DHCP to provide an IP address. For Static IP, select this option and provide an IP address, netmask, and the IP address of the default gateway. |
| **L2TP Server IP/FQDN**         | Enter the name of the server. |
| **Username**                   | The username assigned to you by the ISP. |
| **Password**                   | The password assigned to you by the ISP. |
| **DNS Server**                 | Select **Use L2TP Provided DNS Server** or **Use DNS**. |
| **Static DNS 1 & 2**            | Enter the IP address of the primary and or secondary Static DNS in the fields. |
| **Connect Mode**                | Select **Connect on Demand** if your ISP charges when connected. Enter the maximum idle time, in seconds, to wait before terminating the connection due to inactivity. Default is 5 minutes. Select **Keep Alive** to periodically check the connection, and to re-establish the connection when it is disconnected. |
| **Authentication Type**         | Select the authentication type from the drop-down list (**Auto**, **PAP**, **CHAP**, **MS-CHAP**, **MS-CHAPv2**). |

**When the IPv4 connection uses Bridge**

| **Bridge to**                  | VLAN1 is the default. |
| **IP Address**                 | Enter the IP address. |
| **Netmask**                    | Enter the netmask. |
| **Default Gateway**            | Enter the default gateway. |
| **Static DNS 1 & 2**            | Enter the IP address of the primary and or secondary Static DNS in the fields. |

**When the IPv6 connection uses SLAAC**

In the SLAAC Settings section, enter the following information:

| **DNS Server**                  | Select **Use DNS as Below** from the drop-down list. |
**Static DNS 1 & 2**
Enter the IP address of the primary and or secondary Static DNS in the fields.

**DHCP-PD (IPv6 only)**
Check to enable and enter a prefix name.

---

**Step 6**
To disable IPv6, check Disabled.

**Step 7**
Click Apply.

**For Advanced**

**Step 8**
Click the Advanced tab and configure the following:

<table>
<thead>
<tr>
<th>MTU – Maximum Transmission Unit</th>
<th>Select Auto to set the size automatically. To set the MTU size manually, select Manual and enter the MTU size. (The size in bytes of the largest protocol data unit that the layer can pass.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address Clone</td>
<td>Check MAC Address Clone and enter the MAC address. Click Clone My PC's MAC to use the MAC address of your computer as the clone MAC address for the device.</td>
</tr>
</tbody>
</table>

**Step 9**
Click Apply.

**Note**
Add any of these sub-interfaces to the Multi-WAN table to forward the default route traffic. Or it will only forward the connected route traffic based on the routing table.

---

**Multi-WAN**

WAN failover and load balancing features provide efficient utilization of multiple WAN interfaces. Based on the configuration, this feature can be used to distribute traffic among the interfaces. The Multi-WAN feature provides the outbound WAN traffic, and load balancing over multiple WAN interfaces (WAN & USB) based on a numeric weight assignment. It also monitors each WAN connection using repeated ping tests and automatically routes outbound traffic to another WAN interface if connectivity is lost. The specific outbound traffic rules can also be configured because of 5-tuple of a connection. Outgoing network load-balancing is performed on a per IP connection basis; it is not channel-bonding, where a single connection uses multiple WAN connections simultaneously. The VLAN interfaces of WAN can also be configured for load balance or failover.

To configure the multi WAN settings, follow these steps:

**Step 1**
Select **WAN > Multi-WAN Settings**.

**Step 2**
In the Interface Setting Table, configure the following:

- **Interface** – WAN interface name to apply the load balance and failover configuration. Select and check the desired interface (WAN1, WAN2, USB1, or USB2).
- **Precedence (for Failover)** – Enter the priority value for the interface to bring up another connection on another interface.
- **Weighted by Percentage or Weighted by Bandwidth (for Load-Balance)** – Enter the weight percentage or value for each connection. The interface routes traffic to the secondary connection if the primary connection's is overloaded in an effort to balance the bandwidth load. To ensure full utilization of both connections, the ratio between the connections' load balancing weights should reflect the ratio between the connections' bandwidths.
Step 3
Select an interface and click **Edit** and configure the following as described here:

- **Retry Count** – Number of times to ping a device. The range is 1 to 10 and the default is 3.
- **Retry Timeout** – Number of seconds to wait between the pings. The range is 1 to 300 and the default is 5 seconds.
- **Detect Destination** - Select **Default Gateway** or **Remote Host** and enter the host name to ping this device for network service detection.

Step 4
Click **Apply** to return to the Multi-WAN menu.

Step 5
Next, check **Enable Policy Based Routing** to enable policy based routing.

Step 6
In the Policy Binding Table, click **Add** or **Edit** or **Delete**. Policy Binding requires the interface to be used for specified services. It allows the administrator to bind specific outgoing traffic to a WAN interface. Next, configure the following:

<table>
<thead>
<tr>
<th>Priority</th>
<th>Enter a number for the priority.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP</td>
<td>Enter the source IP address.</td>
</tr>
<tr>
<td>Destination IP</td>
<td>Enter the destination IP address.</td>
</tr>
<tr>
<td>Services</td>
<td>Select a service from the drop-down list. If a service is not listed, you can click <strong>Service Management</strong> to add it.</td>
</tr>
<tr>
<td>Outgoing Interface</td>
<td>Select the outgoing interface (WAN1, WAN2, USB1, or USB2) from the drop-down list.</td>
</tr>
<tr>
<td>Failover to backup WAN</td>
<td>Select <strong>On</strong> or <strong>Off</strong> from the Failover to back up WAN drop-down list. <strong>Note</strong> If you select <strong>Off</strong>, the traffic is dropped when the binding interface goes off line or down.</td>
</tr>
<tr>
<td>Status</td>
<td>Select <strong>Enable</strong> or <strong>Disable</strong> to enable or disable the status of the policy.</td>
</tr>
</tbody>
</table>

Step 7
You can also edit or delete a configuration by clicking **Edit** or **Delete**.

Step 8
Click **Apply**.

**Note** Some service providers do not allow to ping the default gateway. Please choose a valid remote host to detect the network connectivity or simply disable the detection. Otherwise, the traffic will not be forwarded by the device.

---

**Mobile Network**

A mobile broadband modem is a type of modem that allows a device to receive Internet access using a mobile broadband connection instead of using phone or cable lines.

To configure the Mobile Network, follow these steps:

Step 1
Select **WAN > Mobile Network**.

Step 2
In the Global Settings section, select the interface (USB1 or USB2) to apply the settings.

Step 3
In the Card Status section, click the connect icon to establish the connection.
Mobile Network Setup

To configure the Mobile Network Setup, follow these steps:

**Step 1**
In the Configuration Mode, select **Auto** to connect to the network automatically.

**Step 2**
Enter the **SIM PIN** - the pin code associated with your SIM card.

**Step 3**
Or, select **Manual** and to connect to the network manually and configure the following:

- **Access Point Name** – Enter the access point name provided by your mobile network service provider.
- **Dial Number** – Enter the number provided by your mobile network service provider for the Internet connection.
- **Username and Password** – Enter the username and password provided by your mobile network service provider.
- **SIM PIN** – Enter the PIN code associated with your SIM card.
- **Server Name** – Enter the name of the server.
- **Authenticate** – Select the option to authenticate.

**Step 4**
Select one of the following for the Connect Mode.

- **Connect on Demand** – It specifies the connection timers after which the connection is terminated if there is inactivity. Enter the Max Idle Time, in seconds, to wait before terminating the connection due to inactivity. Default is 5 minutes.

- **Keep Alive** – It checks the connection with device periodically, to re-establish the connection when disconnected. In the Redial Period, enter the time in seconds for the device to check the connection automatically. Default period is 30 seconds.

**Step 5**
**HiLink Mode** - Some dongles like the Huawei E8372, support the HiLink mode. You can open the dongle’s configuration page to configure more settings. To configure the HiLink Mode, follow these steps:

a) In the Configuration Mode, select **HiLink** to connect to the dongle.

b) Enter the Card Model number that is associated to your dongle.

c) Click **Open HiLink Page** to configure the settings on your dongle.

d) **Username and Password** – Enter the username and password.

Bandwidth Cap Setting

The Bandwidth Cap Tracking limits the transfer of specified amount of data over a period. It is also known as a band cap or data cap. To configure the Bandwidth Cap Setting, follow these steps:

**Step 1**
Check **Bandwidth Cap Tracking** and enter the following:

- **Monthly Renewal Date** – Select number of days to apply the bandwidth cap settings.
• **Monthly Bandwidth Cap** – Enter the size of the data.

• **Send an email to administrator if 3G/4G usage has reached percentage of monthly bandwidth cap** – Select the percentage of data for monthly bandwidth cap. When the cap is reached, an email alert is sent to the administrator.

Step 2  Click **Apply**.

---

## Dynamic DNS

Dynamic Domain Name System (DDNS) is a method of keeping a domain name linked to a changing IP address since not all computers use static IP addresses. DDNS automatically updates a server in the DNS with the active configuration of its hostnames, addresses, or other information. DDNS assigns a fixed domain name to a dynamic WAN IP address. Hence, you can host your own web FTP, or another type of TCP/IP server on your LAN. There are several DDNS services to choose from, most of which are free, or available at a nominal cost. The most popular is DynDNS.

To configure dynamic DNS policies, follow these steps:

1. Step 1  Select **WAN > Dynamic DNS**.
2. Step 2  In the Dynamic DNS Table, select the interface (**WAN1, WAN2, USB1, or USB2**) to add to the Dynamic DNS policy.
3. Step 3  Click **Edit**.
4. Step 4  Check **Enable this Dynamic DNS policy** to enable the policy configuration.
5. Step 5  Select the name of service provider from the Provider drop-down list.
6. Step 6  Enter a **Username** and **Password** for the DDNS account.
7. Step 7  Enter the full name of the device including the domain name in Fully Qualified Domain Name.
8. Step 8  Check **Enable** to receive updates to Dynamic DNS provider and select the periodicity.
9. Step 9  Click **Apply**.
10. Step 10 Click **Refresh** to refresh the Dynamic DNS Table.

---

## Hardware DMZ

A Demilitarized Zone (DMZ) accepts all incoming traffic and allows all outgoing traffic. A DMZ is a subnetwork that is open to the public but behind the firewall. A DMZ allows you to redirect packets entering your WAN port to a specific IP address. You can configure the firewall rules to allow access to specific services and ports in the DMZ from both the LAN and WAN. If there is an attack on any of the DMZ nodes, the LAN is not necessarily vulnerable. We recommend that you place hosts that must be exposed to the WAN (such as web or email servers) in the DMZ network.

To configure the hardware DMZ configuration, follow these steps:

1. Step 1  Select **WAN > Hardware DMZ**.
2. Step 2  Click **Enable** to change the LAN4 to DMZ port.
IPv6 Transition

For migrating from IPv4 to IPv6, you can use an Internet transition mechanism called 6in4. The 6in4 uses tunneling to encapsulate IPv6 traffic over configured IPv4 links. The 6in4 traffic is sent over the IPv4, in which the IPv4 packet header. This is followed by the IPv6 packet whose IP headers have the IP protocol number set to 41.

To configure the IPv6 transition, follow these steps:

**Step 1** Select WAN > IPv6 Transition.
**Step 2** In the Tunnel Table, select the interface to be configured and click Edit.
**Step 3** Check Enable.
**Step 4** Enter the description.
**Step 5** Select the Local Interface from the drop-down list (WAN1 or WAN 2).
**Step 6** Local IPv4 Address displays the address of the selected interface.

IPv6 in IPv4 Tunnel (6in4)

To add IPv4 Tunnel (6in4), enter the following information:

**Step 1** Click the IPv6 in IPv4 Tunnel (6in4) tab.
**Step 2** Enter the Remote IPv4 Address.
**Step 3** Enter the Local IPv6 Address.
**Step 4** Enter the Remote IPv6 Address.
**Step 5** Click Apply.

IPv6 Rapid Deployment (6rd)

In IPv6 Rapid Deployment (6rd), each ISP uses one of its own IPv6 prefixes instead of the special 2002::/16 prefix standardized for 6to4. Hence, a provider is guaranteed for its 6rd hosts availability from all native IPv6 hosts that can reach their IPv6 network.

To add IPv6 Rapid Deployment (6rd), enter the following information:

**Step 1** Click the IPv6 Rapid Deployment (6rd) tab.
Step 2  
Click **Automatically from DHCP** to use the DHCP (option 212) to obtain 6rd Prefix, Relay IPv4 Address, and IPv4 Mask Length.

Step 3  
Or, select **Manual** and set the following 6rd parameters.

a) Enter the **IPv4 Address of Relay**.

b) Enter the **IPv4 Common Prefix Length**.

c) Enter the **IPv6 Prefix/Length**. The IPv6 network (subnetwork) is identified by the prefix. All hosts in the network have the identical initial bits for their IPv6 address. Enter the number of common initial bits in the network addresses. Default is 64.

Step 4  
Click **Apply**.
A local area network (LAN) is a computer network that spans within a relatively small area close to each other, such as in an office building, a school, or a home. LANs are characterized by their topology, protocols, and media.

A LAN is useful for sharing resources like files, printers, games, or other applications. A LAN often connects to other LANs, the Internet, or another WAN. This section contains the following topics:

- Port Settings, on page 51
- VLAN Settings, on page 52
- LAN/DHCP Settings, on page 53
- Static DHCP, on page 55
- 802.1X Configuration, on page 55
- DNS Local Database, on page 56
- Router Advertisement, on page 56

## Port Settings

The Port Settings page displays the ports for EEE, Flow Control, Mode, Port Mirror, and Link Aggregation.

To configure the port settings for the LAN, follow these steps:

**Step 1** Select **LAN > Port Settings**.

**Step 2** In the Basic Per Port Configuration table, configure the following:

<table>
<thead>
<tr>
<th>Port Label</th>
<th>Enter the name of the port.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Check to enable the port to allow the settings. When this check box is disabled, all settings on the port are lost.</td>
</tr>
<tr>
<td>EEE (Energy Efficient on Ethernet)</td>
<td>Check to allow port to consume less power during period of low data activity.</td>
</tr>
<tr>
<td>Flow Control</td>
<td>Check to enable to symmetric flow control. Flow control is used to send pause frames and respecting pause frames to and from the LAN PC connected to the device.</td>
</tr>
<tr>
<td>Mode</td>
<td>Select the port setting mode from the drop-down list.</td>
</tr>
</tbody>
</table>

**Step 3** In the Port Mirror Configuration section, enter the following information:
VLAN Settings

Traffic on the port can be tagged by applying a specified VLAN. This tagging can help in differentiating the traffic and forwarding it. There are only 32 VLANs in the system. If there are few VLANs used by WAN, then LAN can use rest of them.

To configure the VLAN settings, enter the following information:

**Step 1** Select **LAN > VLAN Settings**.
**Step 2** In the VLAN Table, click **Add**.
**Step 3** Enter the VLAN ID.
**Step 4** Check to enable the Inter-VLAN routing and the Device Management.
**Step 5** For the IPv4, enter the IPv4 address and subnet mask.
**Step 6** For the IPv6, enter the Prefix, Prefix Length, and Interface Identifier.
**Step 7** Then, select the DHCP type (**Disabled**, **Server** or **Relay**) for both the IPv4 and IPv6.
**Step 8** Click **Edit** or **Delete** to edit or delete the VLAN table configurations.
**Step 9** In the Assign VLANs to ports table, click **Edit** to assign a VLAN to a LAN port. Specify the following information for each of the VLAN listed in the table.

- **Untagged** – Select **Untagged** from the drop-down list to untag the port.
- **Tagged** – Select **Tagged** from the drop-down list, to include the port as a member for the selected VLAN. Packets sent from this port destined to the chosen VLAN will have the packets tagged with the VLAN ID. If there are no untagged VLANs on a port, the interface automatically joins the VLAN1.
- **Excluded** – Select **Excluded** from the drop-down list, to exclude the port from the selected VLAN. When the untagged VLANs are excluded from a port, the port automatically joins the default VLAN.

**Step 10**
Click **Apply**.

---

## LAN/DHCP Settings

DHCP setup configures the DHCP server for relay or Option 82 (DHCP relay agent information option) for LAN clients to obtain IP addresses. DHCP server maintains local pools and leases. It also allows LAN clients to connect to a remote server for obtaining IP address.

Option 43 and 82 enable a DHCP relay agent to include information about itself when forwarding client-originated DHCP packets to a DHCP server. The DHCP server can use this information to implement IP addressing or other parameter-assignment policies.

To configure the LAN/DHCP settings, follow these steps:

### Step 1
Select **LAN > LAN/DHCP Settings**.

### Step 2
In the LAN/DHCP Settings Table click **Add**.

### Step 3
Select **Interface**, and click **Next**.

### Step 4
To configure the DHCP for IPv4, select the DHCP type for IPv4.

<table>
<thead>
<tr>
<th>Disabled</th>
<th>Disables the DHCP server for IPv4 on this device. There are no additional parameters to complete.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>The DHCP server assigns addresses to clients from their respective pools.</td>
</tr>
<tr>
<td>Relay</td>
<td>Sends the DHCP requests and replies from another DHCP server through the device. Enter the remote DHCP server IPv4 address to configure DHCP relay agent.</td>
</tr>
</tbody>
</table>

### Configuring DHCP for IPv4

**Step 5**
Click **Next** and configure the following:

<table>
<thead>
<tr>
<th><strong>Client Lease Time</strong></th>
<th>Amount of time (in minutes) that a network user is allowed to connect to the device with the current IP address. Valid values are 5 to 43,200 minutes. The default is 1440 minutes (equal to 24 hours).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Range Start and Range End</strong></td>
<td>The range start and end of IP addresses that can be assigned dynamically. The range can be up to the maximum number of IP addresses that the server can assign without overlapping the PPTP and SSL VPN.</td>
</tr>
<tr>
<td><strong>DNS Server</strong></td>
<td>DNS service type; where the DNS server IP address is acquired.</td>
</tr>
<tr>
<td><strong>Static DNS 1 and Static DNS 2</strong></td>
<td>Static IP address of a DNS Server. (Optional) If you enter a second DNS server, the device uses the first DNS server to respond to a request.</td>
</tr>
<tr>
<td><strong>WINS Server</strong></td>
<td>Optional IP address of a Windows Internet Naming Service (WINS) server that resolves NetBIOS names to IP addresses. Default is 0.0.0.0.</td>
</tr>
</tbody>
</table>
DHCP Options

- **Option 66** – Enter the IP address or the hostname of a single TFTP server.
- **Option 150** – Enter the IP addresses of a list of TFTP servers.
- **Option 67** – Enter the boot filename.
- **Option 43** – Enter the vendor specific information. For example, specify the PnP address with these strings “5A1N;K4;B2;I10.10.10.10;J80”.

**Configuring DHCP type for IPv6**

**Step 6**
To configure the DHCP Mode for IPv6, enter the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Disable</strong></td>
<td>Disables the DHCP on this device. There are no additional parameters to complete.</td>
</tr>
<tr>
<td><strong>Server</strong></td>
<td>DHCP server that assigns addresses to clients from their respective pools.</td>
</tr>
</tbody>
</table>

**Step 7**
Click Next and configure the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Client Lease Time</strong></td>
<td>Amount of time that a network user is allowed to connect to the device with the current IP address. Enter the amount of time in minutes. Valid values are 5 to 3200 minutes. Default is 1460 minutes (24 hours).</td>
</tr>
<tr>
<td><strong>Range Start</strong></td>
<td>Starting address of the IPv6 address pool.</td>
</tr>
<tr>
<td><strong>Range End</strong></td>
<td>Ending address of the IPv6 address pool.</td>
</tr>
<tr>
<td><strong>DNS Server</strong></td>
<td>Type of DNS (server static), proxy, or the DNS server provided by your ISP.</td>
</tr>
<tr>
<td><strong>Static DNS1 and DNS2</strong></td>
<td>(Optional) IP address of a DNS server. If you enter a second DNS server, the device uses the first DNS server to respond. Specifying a DNS server can provide faster access than using a DNS server that is dynamically assigned. Default is 0.0.0.0.</td>
</tr>
</tbody>
</table>

**Configuring Option 82 Circuit**

**Step 8**
To configure the Option 82 Circuit enter the following information:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Enter description for option 82 client.</td>
</tr>
<tr>
<td><strong>Circuit ID/ASCII</strong></td>
<td>Enhances the validation security to determine about the information which is provided in the Option 82 Circuit ID. Enter the circuit ID and select its format from the drop-down list.</td>
</tr>
<tr>
<td><strong>Bitmask</strong></td>
<td>If you select HEX as the format for the Circuit ID/ASCII, enter the bitmask.</td>
</tr>
</tbody>
</table>

**Step 9**
Click Next and enter the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP Address &amp; Subnet Mask</strong></td>
<td>Enter the IP address and subnet mask of the device.</td>
</tr>
</tbody>
</table>

**Step 10**
Click Next.

**Step 11**
To add a new DHCP Configuration, configure the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Client Lease Time</strong></td>
<td>Amount of time that a network user is allowed to connect to the device with the current IP address. Enter the amount of time in minutes. Valid values are 5 to 3200 minutes. Default is 1460 minutes (24 hours).</td>
</tr>
</tbody>
</table>
The range start and end of IP addresses that can be assigned dynamically. The range can be up to the maximum number of IP addresses that the server can assign without overlapping the PPTP and SSL VPN. For example, if the device uses the default LAN IP address, 192.168.1.1, the starting value must be 192.168.1.2 or greater.

### DNS Server
- DNS service type; where the DNS server IP address is acquired.

### Static DNS 1 and Static DNS 2
- Static IP address of a DNS Server. (Optional) if you enter a second DNS server, the device uses the first DNS server to respond to a request.

### WINS Server
- Optional IP address of a Windows Internet Naming Service (WINS) server that resolves NetBIOS names to IP addresses. Default is 0.0.0.0.

### DHCP Options
- **Option 66** – Enter the IP address or the hostname of a single TFTP server.
- **Option 150** – Enter the IP addresses of a list of TFTP servers.
- **Option 67** – Enter the boot filename.

---

### Step 12
Click **Ok**, then click **Apply**.

---

## Static DHCP

Static DHCP allows an IPv4 address to the defined MAC.

To configure static DHCP follow these steps:

### Step 1
Select **LAN > Static DHCP**.

### Step 2
Click **Add**.

### Step 3
In the Static DHCP Table, enter a name in the Name field.

### Step 4
Enter the IPv4 and MAC addresses in the respective fields.

### Step 5
Check **Enable**.

### Step 6
Click **Apply**.

---

## 802.1X Configuration

The IEEE 802.1X port-based authentication prevents unauthorized devices (clients) from gaining access to the network. This network access control uses the physical access characteristics of the IEEE 802 LAN infrastructures to authenticate and authorize devices attached to a LAN port, that has point-to-point connection characteristics. A port in this context is a single point of attachment to the LAN infrastructure.

The device supports multiple-hosts mode. In this mode, only one of the attached hosts must be successfully authorized for all hosts to be granted network access. If the port becomes unauthorized (re-authorization fails or an EAPOL-logoff message is received), all attached clients are denied access to the network.

To configure port-based authentication:
Step 1  Select LAN > 802.1X Configuration.
Step 2  Check Enable Port-Based Authentication to enable the feature.

Note  802.1X requires the use of RADIUS for authentication. Ensure that the RADIUS server is defined in User Accounts, on page 29.

Step 3  Select the Administration Status in the 802.1X Configuration Table from the drop-down list.

• Force Authorized – Authorization is not needed. At least one LAN port must be force authorized.

• Auto – Enables port-based authentication. The interface moves between an authorized or unauthorized state based on the authentication exchange between the device and the client.

Step 4  Click Apply.

Note  Ensure that the respective configuration is active and correct before enabling a Port-based authentication.

DNS Local Database

A local Domain Name Service (DNS) server, is used for accelerated DNS service response. DNS matches a domain name to its routable IP address. For commonly used domain names a DNS local database which acts as a local DNS server can give faster results than using an external DNS server. If a requested domain name is not found in the local database, the request is forwarded to the DNS server that is specified on the Setup.

If you enable this feature, configure the client devices to use the device as the DNS server. By default, Windows computers are set to obtain a DNS server address automatically from the default gateway.

To change the TCP/IP connection settings, for example, on a PC running Windows, follow these steps:

1. Go to the Local Area Connection Properties > Internet Protocol > TCP/IP Properties.

2. Choose Use the following DNS server address.

3. Enter the LAN IP address of the device as the Preferred DNS Server.

To add a new host, follow these steps:

Step 1  Select LAN > DNS Local Database.
Step 2  Click Add and enter the host name and IPv4 or IPv6 address. You can also edit or delete a DNS.
Step 3  Click Apply.

Router Advertisement

The Router Advertisement Daemon (RADVD) is used for defining interface settings, prefixes, routes, and announcements. Hosts rely on the devices on their local networks to facilitate communication to all other hosts except those on the local network. The devices send and respond to the Router Advertisement messages
regularly. By enabling this feature, messages are sent by the router periodically and in response to solicitations. A host uses the information to learn the prefixes and parameters for the local network. Disabling this feature effectively disables auto configuration, requiring manual configuration of the IPv6 address, subnet prefix, and default gateway on each device.

To configure the Router Advertisement, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Select LAN &gt; Router Advertisement.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select the VLAN ID from the drop-down list.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Check Enable to enable router advertisement and configure the following:</td>
</tr>
</tbody>
</table>

**| **Advertisement Mode | Select the advertisement mode from the drop-down list (Unicast or Unsolicited Multicast). |
| Advertisement Interval | Enter the time interval between 10 and 1800 (Default is 30 seconds) at which the router advertisement messages are sent. |
| RA Flags | Determines whether hosts can use DHCPv6 to obtain IP addresses and related information. Select and check one of the following:  
  • Managed – Hosts use an administered, stateful configuration protocol (DHCPv6) to obtain stateful addresses and other information through DHCPv6.  
  • Other – Uses an administered, stateful configuration protocol (DHCPv6) to obtain other, non-address information, such as DNS server address. |
| Router Preference | Preference metric used in a network topology where multi-homed hosts have access to multiple routers. Router Preference helps a host to choose an appropriate device. There are three preferences to choose from, such as **High**, **Medium**, or **Low**. The default setting is High. Select the preference from the drop-down list. |
| Maximum Transmission Unit (MTU) | The MTU is the size of the largest packet that can be sent over the network. It is used in the router advertisement messages to ensure that all nodes on the network use the same MTU value when the LAN MTU is not well-known. The default setting is 1500 bytes, which is the standard value for Ethernet networks. For PPPoE connections, the standard is 1492 bytes. Unless your ISP requires a different setting, this setting should not be changed. Enter a value between 1280 and 1500. |
| Router Lifetime | Enter the time in seconds for the router advertisement messages to exist on the route. The default is 3600 seconds. |

**Step 4** In the Prefix Table, click **Add** and enter a name for the prefix.  
**Step 5** Enter the prefix length and the lifetime in the Prefix Length and Lifetime fields.  
**Step 6** Click **Apply**.
Wireless (RV340W)

A Wireless Local Area Network (WLAN) is a wireless distribution method that implements a flexible data communication system using high-frequency radio waves and often includes an access point to the Internet. This is achieved by augmenting, rather than replacing a wired LAN within a building or campus. Since the WLANs use radio frequency to transmit and receive data, they don't require a wired connections. This allows users to move around the coverage area, and still maintain a network connection.

This section describes the WLAN, which is a type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes and contains the following topics:

- Basic Settings, on page 59
- Advanced Settings, on page 62
- Captive Portal, on page 63
- WPS, on page 65

Basic Settings

The RV340W provides Wireless LAN (WLAN), with all ports (LAN and WLAN) on single broadcast domain. The device supports 802.11ac standard and concurrent dual-band selection at 2.4 GHz and 5 GHz. Depending on the radio, you can select the frequency or channel for WLAN network data transmission and reception. Selecting the appropriate channel width for each radio can improve the WLAN throughput.

In Basic Settings, you can add, edit, or delete the wireless SSID settings, and select and configure the radio channels. You can add up to four separate virtual wireless networks per Radio. In other words, you cannot add more than eight SSIDs (that is, four SSIDs per radio); the Add button will be grayed out when you reach this limit.

To configure the Wireless SSID settings, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Select Wireless &gt; Basic Settings.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Under the Wireless Table, click Add or Edit.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Next, in the Add/Edit Wireless SSID Settings page, configure the following:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SSID Name</th>
<th>Specify the name of the network.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>Check Enable to enable the network.</td>
</tr>
<tr>
<td><strong>Actively applied to Radio</strong></td>
<td>Select 2.4G or 5G band to connect only to a network matching both network settings and band selection. The SSID will be created on the radio selected. Select <strong>Both</strong> to configure the SSID on both the radios and connect this profile to an available network with matching network settings.</td>
</tr>
<tr>
<td><strong>SSID Broadcast</strong></td>
<td>Check to enable SSID broadcasting if you want to allow wireless clients within range to detect this wireless network when scanning for available networks. Disable this feature if you do not want to make the SSID known. If disabled, wireless clients can connect to your wireless network only if they provide the SSID and the required security credentials.</td>
</tr>
</tbody>
</table>
| **Security Mode** | Choose a security mode for the network from the following:  
- **None**: Select this option for no security.  
- **WEP-64**: Select the 64-bit WEP security mode and enter a WEP Key if you are using old equipment that does not support WPA or WPA2 security. The WEP key should be a string of 10 hexadecimal characters.  
- **WEP-128**: Select the 128-bit WEP security mode and enter a WEP Key if you are using old equipment that does not support WPA or WPA2 security. The WEP Key should be a string of 26 hexadecimal characters.  
- **WPA2-Personal**: Select Wi-Fi Protected Access II (WPA2) security protocol for stronger security. If selected, enter an alphanumeric pass phrase.  
- **WPA-WPA2-Personal**: Select this security protocol for stronger security when you allow both WPA and WPA2 clients to connect simultaneously. If selected, enter an alphanumeric pass phrase.  
- **WPA2-Enterprise**: Select this security protocol to use RADIUS server authentication. If selected, specify the following:  
  - **Radius Server IP Address** (handles client authentication).  
  - **Radius Server Port** (port used to access the RADIUS server).  
  - **Radius Secret** (shared RADIUS secret).  
- **WPA-WPA2-Enterprise**: Select this security protocol to use the RADIUS server authentication when you allow both WPA and WPA2 clients to connect simultaneously. If selected, specify the Radius Server IP Address, Radius Server Port, and Radius Secret. |
| **Wireless Isolation with SSID** | Check **Enable** to enable wireless isolation within the SSID. When wireless isolation is configured, wireless clients will not be able to see or communicate with each other when connected to the same SSID. |
| **WMM** | To prioritize and queue the traffic according to the Access Category (AC), check **Enable** to enable the Wireless Multimedia Extensions (WME). Enabling WME may result in more efficient throughput, but higher error rates within a noisy Radio Frequency (RF) environment. |
| **WPS** | Check to enable Wi-Fi Protected Setup (WPS). It allows up to two usage modes: PIN and Push Button. If enabled, click **Configure** and set up the WPS parameters in the pop-up. For more information on configuring WPS, see **WPS, on page 65**. |
VLAN | Specify the VLAN ID, the SSID should be mapped to. Devices connecting to this network are assigned addresses on this VLAN. The default VLAN ID is 1 and if all the devices are on the same network, this can be left unchanged.

Max Associated Clients | Specify the maximum number of clients to be associated simultaneously (50 for 2.4G and 124 for 5G, per SSID, by default).  
**Note** | The sum of the configured Max Associated Clients of all enabled SSIDs should not exceed 50 clients for 2.4G and 124 for 5G (128 when MU-MIMO is enabled).

Time of Day Access | Specify the time period if the SSID shall be available only for certain hours every day or for certain days in every week. Thus, you can further protect your network, by specifying when users can access the network, thereby restricting access to it.

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. Check to enable MAC filtering for the SSID. If enabled, click **Configure** and specify the MAC blacklist (devices to be prevented from accessing) and whitelist (devices to be permitted to access) for the wireless network.

Captive Portal | Check to enable Captive Portal verification for the SSID and select a portal profile from the drop-down list. If enabled, you can also click **New** and configure a new profile. See **Captive Portal, on page 63** for more information on adding a new Captive Portal Profile.

**Step 4** Click **Apply**.

---

**Configuring 2.4 GHz Radio**

You can enable or disable the dual-band frequencies — 2.4 GHz and 5 GHz — that are supported by the device. You can also specify the channel number for each band or choose **Auto Channel Selection**. These settings will be applied to all virtual wireless networks. Depending on the radio selected, the WLAN network transmits and receives data on the specific frequency, or channel selected. Selecting an appropriate channel width for each radio can improve the WLAN throughput.

To configure the concurrent channel selection parameters, follow these steps:

**Configuring 2.4 GHz Radio**

**Step 1** Click **Wireless > Basic Settings > 2.4G**.

**Step 2** Check **Enable** to enable the radio 2.4 GHz band.

**Step 3** Select the network band mode (**B Only, G Only, N Only, B/G-Mixed, G/N-Mixed, or B/G/N-Mixed**) from the Wireless Network Mode drop-down list.

**Step 4** Check **20 MHz** or **20/40 MHz** to select the channel bandwidth.

**Step 5** Select the primary channel by clicking the lower or upper radio button.

**Note** You cannot select a primary channel if you have selected **20 MHz bandwidth** in Step 4 or **Auto** from the drop-down list.
Configuring 5 GHz Radio

To configure the 5 GHz radio, follow these steps:

**Step 1** Click Wireless > Basic Settings > 5G.

**Step 2** Check Enable to enable the radio 5 GHz band.

**Step 3** Select the network band mode (A Only, N/AC-Mixed, or A/N/AC-Mixed) from the Wireless Network Mode drop-down list.

**Step 4** Click the 20 MHz, 40 MHz, or 80 MHz radio button to select the channel bandwidth.

**Step 5** Select the primary channel by clicking Lower or Upper.

*Note* You can select a primary channel, only if you have selected 40 MHz bandwidth.

**Step 6** Select an appropriate wireless channel from the drop-down list. You may select Auto and let the system select the channel.

**Step 7** To enable the Unscheduled Automatic Power Save Delivery (U-APSD) mode, and allow the connected clients that have U-APSD feature, to save power, check U-APSD (WMM Power Save). This uses mechanisms from 802.11e and legacy 802.11 to save power and fine-tune power consumption.

**Step 8** Click Apply.

Advanced Settings

For each radio, you can specify the advanced settings, such as Frame Burst, WMM No Acknowledgment, Basic Rate, Transmission Rate, DTIM Interval, RTS Threshold, etc.

To configure the advanced settings under Wireless, follow these steps:

**Step 1** Click Wireless > Advanced Settings > 2.4G or 5G tab.

**Step 2** Configure the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frame Burst</td>
<td>Check Enable to enable sending multiple frames with minimum inter-frame gap that enhances network efficiency and reduces overhead.</td>
</tr>
</tbody>
</table>
Check Enable to achieve efficient throughput. This may result in higher error rates in a noisy Radio Frequency (RF) environment.

**Data Rate**
For Data Rate, click **Set to Default**, to select default values for the basic and transmission rates.

**Basic Rate**
Select the Basic Rate settings — the 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.

**Transmission Rate**
Select the Transmission Rate settings — the rate of data transmission depending on the speed of your wireless network.

**CTS Protection Mode**
Clear-To-Send (CTS) Protection Mode is the mechanism used by the 802.11 wireless networking protocol to reduce frame collisions caused by the hidden node problems. By default, this is set to **Auto**. To disable it, click **Disabled**.

**Beacon Interval**
Specify the Beacon Interval (the time interval between beacon transmissions) in milliseconds. A beacon is a packet broadcast by the device to synchronize the wireless network and the time at which a node (like an AP) must send a beacon is known as Target Beacon Transmission Time (TBIT), expressed in Time Unit (TU). The range is 40 to 3500 milliseconds, default is 100.

**DTIM Interval**
Specify the Delivery Traffic Indication Map (DTIM Interval). This informs the clients about the presence of buffered multicast/broadcast data on the Access Point. It is generated within the periodic beacon at a frequency specified by the DTIM Interval. The range is 1 to 255, default is 1.

**Fragmentation Threshold**
Enter the Fragmentation Threshold value that 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. The range is 256 to 2346, default is 2346.

**RTS Threshold**
In the RTS Threshold field, enter the Request-To-Send (RTS) threshold size. If a network packet is smaller than the specified threshold size, the RTS/CTS mechanism will not be enabled. The range is 0 to 2347, default is 2347.

**Tx Power**
Select the volume of data to be transmitted from the drop-down list.

**Step 3**
Click **Apply**.

---

**Captive Portal**

The Captive Portal feature provides clients, with a controlled and authenticated access to network resources, without compromising security. In other words, a client connecting to the WLAN interfaces is limited to a “walled garden” until authorized. The captive portal displays a special web page to authenticate clients before they can use the Internet. The client can resolve DNS and web browser websites specifically added to such a “walled garden”. Authentication uses a captive portal that initiates authentication. When an unauthenticated
client tries to connect to a web page (on port 80), the request is intercepted by a daemon and redirected to the captive portal (UI port)

You can configure Captive Portal for each virtual wireless network on your device by associating it with a portal profile. You can also view the Captive Portal status by choosing Status and Statistics > Captive Portal Status. See Basic Settings, on page 59 for instructions on how to enable a Captive Portal profile.

To create Captive Portal Profile:

**Step 1** Click Wireless > Captive Portal.

**Step 2** On the Captive Portal page, click Add under Portal Profile Table. To modify an existing Portal Profile, check the corresponding check box and click Edit.

**Step 3** On the Add Captive Portal Profile page, configure the following:

<table>
<thead>
<tr>
<th>Profile Name</th>
<th>Enter a name for the new Captive Portal profile.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>Choose if you want to enable (Auth) or disable (No Auth) authentication.</td>
</tr>
<tr>
<td>After user login, redirect to</td>
<td>Select Original URL, or A New URL and enter the URL in the text field, to redirect users to a URL after authentication.</td>
</tr>
<tr>
<td>Idle Timeout</td>
<td>Set the lifetime of the authentication in seconds, ranging from 0-1440. 0 indicates infinite time.</td>
</tr>
</tbody>
</table>

**Step 4** In the Portal Page Customization section, configure the following:

<table>
<thead>
<tr>
<th>Font Color</th>
<th>Select a font color, from the drop-down list, for the text you want to display on the page.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Background Picture</td>
<td>Click Browse and select an image to be displayed as the background of the portal page.</td>
</tr>
<tr>
<td>Company Name</td>
<td>Specify the company name to be displayed.</td>
</tr>
<tr>
<td>Company Logo Picture</td>
<td>Click Browse and select the image of the company logo to be displayed.</td>
</tr>
<tr>
<td>Welcome Message</td>
<td>Enter the welcome message to be displayed at login.</td>
</tr>
<tr>
<td>Username Field</td>
<td>Enter the text for user name field.</td>
</tr>
<tr>
<td>Password Field</td>
<td>Enter the text for password field.</td>
</tr>
<tr>
<td>Login Button Name</td>
<td>Enter the text displayed on the login button.</td>
</tr>
<tr>
<td>Copyright Message</td>
<td>Enter standard Copyright text associated with your company.</td>
</tr>
<tr>
<td>Error Message for Authentication Failure</td>
<td>Enter the text for the error message for authentication failure.</td>
</tr>
<tr>
<td>Show Agreement</td>
<td>Check Show Agreement to accept the terms of use.</td>
</tr>
<tr>
<td>Agreement Title</td>
<td>Enter a title for the Agreement text.</td>
</tr>
<tr>
<td>Agreement Message</td>
<td>Enter the Agreement terms to be displayed.</td>
</tr>
</tbody>
</table>

**Step 5** Click Apply.
WPS

Wi-Fi Protected Setup (WPS) is a network security feature that allows WPS-enabled clients to easily and securely connect to the wireless network. There are three methods to connect to the wireless network that are supported by WPS: WPS push button, WPS PIN number through your client’s device, and Device PIN number generated on the WPS configuration page.

To configure WPS:

Step 1
Click Wireless > WPS. The Wi-Fi Protected Setup page appears.

Step 2
Select the SSID (for which the WPS is to be configured) from the WPS drop-down list.

Step 3
Select the radio band (2.4G, 5G, or Both) from the radio drop-down list.

Step 4
Configure the WPS on client devices in one of the following three methods:

a) Click WPS on the client, and then click WPS on this WPS configuration page.
b) If your client device has a WPS PIN number, enter the number in the text field and then click Register.
c) If the client device requires a PIN number from your device, click Generate and enter the PIN number.

In the PIN Lifetime field, choose the desired lifetime of the key. If the time expires, a new key is negotiated.

This completes the WPS configuration.
CHAPTER 8

Routing

This section describes routing, which is the process of selecting the best paths in a network. Dynamic routing is a networking technique that provides optimal data routing. Dynamic routing enables devices to select paths according to real-time logical network layout changes. The device’s routing protocol is responsible for the creation, maintenance, and updating of the dynamic routing table in the dynamic routing. This section contains the following topics:

- IGMP Proxy, on page 67
- RIP, on page 68
- Static Routing, on page 69

IGMP Proxy

The Internet Group Management Protocol (IGMP) is used by hosts and devices on an IP network to create multicast group memberships. IGMP can be used for resources of web and support applications like online streaming for videos and games. The IGMP proxy enables the device to issue IGMP messages on behalf of the clients behind it.

To enable the IGMP proxy follow these steps:

Step 1 Select Routing > IGMP Proxy.
Step 2 Check Enable IGMP Proxy to allow the device and the nodes to communicate with each other.
Step 3 Select the Upstream Interface from the drop-down list.

- **WAN-Auto** – The device can support multi-WAN. If selecting the WAN auto mode, the device will select the active WAN as the upstream port. If multiple WANs are up and work in load balance mode, the WAN port with the lowest port number will be the upstream port. For example, if WAN1 and WAN2 are in load-balance mode, the WAN1 will be the upstream port. If WAN1 is down, the WAN 2 will be the upstream port.

- **Fixed Interface** – The fixed interface will always use the selected port as the upstream port even if it is down. For example, if WAN1 and WAN2 are in load balance mode, and you select WAN 2 as the upstream port, the WAN1 will not receive the multicast traffic regardless of whether the WAN2 is up or down. If selecting the Fixed Interface, make sure to also choose between WAN 1, WAN 2 or VLAN1.

Step 4 Select the Downstream Interface, WAN or VLAN1.
Step 5  Click **Apply**.

---

**RIP**

Routing Information Protocol (RIP) is the standard IGP that is used on Local Area Networks (LAN). RIP ensure a higher degree of network stability by quickly rerouting network packets if one of the network connections goes off-line. When RIP is active, users experience little to no service interruptions due to single device, switch, or server outages if there are sufficient network resources available.

To configure RIP, follow these steps:

---

**Step 1**  Select **Routing > RIP**.

**Step 2**  To enable RIP, check **Enable RIP for IPv4** or **for IPv6** or both and configure the following:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interface</strong></td>
<td>Check <strong>Enable</strong> in the corresponding Interface to allow routes from upstream to be received.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Checking <strong>Enable</strong> for an interface automatically checks RIP version 1, RIP version 2, RIPng (IPv6), and Authentication for that interface. Similarly, unchecking <strong>Enable</strong> unchecks all.</td>
</tr>
<tr>
<td><strong>RIP version 1</strong></td>
<td>This protocol uses classful routing and does not include subnet information or authentication.</td>
</tr>
<tr>
<td></td>
<td>• Check <strong>Enable</strong> to enable sending and receiving routing information on RIP version 1.</td>
</tr>
<tr>
<td></td>
<td>• Check <strong>Passive</strong> to disable routing information from being sent on RIP version 1.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Passive configuration is activated only when <strong>Enable</strong> is checked.</td>
</tr>
<tr>
<td><strong>RIP version 2</strong></td>
<td>This is a classless protocol that uses multicast and has a password authentication.</td>
</tr>
<tr>
<td></td>
<td>• Check <strong>Enable</strong> to enable sending and receiving routing information on RIP version 2.</td>
</tr>
<tr>
<td></td>
<td>• Check <strong>Passive</strong> to disable routing information from being sent on RIP version 2.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Passive configuration is activated only when <strong>Enable</strong> is checked.</td>
</tr>
<tr>
<td><strong>RIPng (IPv6)</strong></td>
<td>Routing Information Protocol next generation (RIPng) uses User Datagram Packets (UDP) to send routing information. This is based on RIP version 2 but used for IPv6 routing.</td>
</tr>
<tr>
<td></td>
<td>• Check <strong>Enable</strong> to enable RIP IPv6 routing.</td>
</tr>
<tr>
<td></td>
<td>• Check <strong>Passive</strong> to disable sending RIPng version.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Passive configuration is activated only when <strong>Enable</strong> is checked.</td>
</tr>
</tbody>
</table>
### Authentication

This is a security feature that forces authentication of RIP packets before routes are exchanged with other devices. This is not available for RIPv1.

- Check **Enable** to enable authentication so that routes are exchanged only with trusted devices on the network.
- **Password**: Select the authentication type — **Plain** (common method of authentication) or **MD5** (challenge-response authentication mechanism) — and enter the password.

---

**Step 3**  
Click **Apply**.

---

### Static Routing

Static Routing is a manually configured fixed pathway that a packet must travel to reach a destination. If there is no communication between the devices on the current network topology, static routing can be configured to communicate between the devices. Static Routing uses less network resources than dynamic routing because they do not constantly calculate the next route to take.

To configure static routing, follow these steps:

**Step 1**  
Select **Routing > Static Routing**.

**Step 2**  
For IPv4 Routes, in the Route Table, click **Add** or **Edit** and configure the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network</strong></td>
<td>Enter the destination subnetwork IP address to which you want to assign a static route to.</td>
</tr>
<tr>
<td><strong>Mask</strong></td>
<td>Enter the subnet mask of the destination address.</td>
</tr>
<tr>
<td><strong>Next Hop</strong></td>
<td>Enter the IP address of the device of the last resort.</td>
</tr>
<tr>
<td><strong>Hop Count</strong></td>
<td>Enter the maximum number of nodes or hops that a packet should pass through before it is discarded. A node can be a device on the network, such as a switch or device.</td>
</tr>
<tr>
<td><strong>Metric</strong></td>
<td>Enter the number of routing algorithms to determine the optimal route for sending network traffic.</td>
</tr>
<tr>
<td><strong>Interface</strong></td>
<td>Choose the interface to use for this static route from the drop-down list.</td>
</tr>
</tbody>
</table>

**Step 3**  
Click **Apply**.

**Step 4**  
For IPv6 Routes, in the Route Table, click **Add** or **Edit** and configure the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Prefix</strong></td>
<td>Enter the IPv6 prefix.</td>
</tr>
<tr>
<td><strong>Length</strong></td>
<td>Enter the number of prefix bits of the IP address.</td>
</tr>
<tr>
<td><strong>Next Hop</strong></td>
<td>Enter the IP address of the device of the last resort.</td>
</tr>
<tr>
<td><strong>Metric</strong></td>
<td>Enter the number of routing algorithms to determine the optimal route for sending network traffic.</td>
</tr>
<tr>
<td>Interface</td>
<td>Choose the interface to use for this static route from the drop-down list.</td>
</tr>
</tbody>
</table>

**Step 5**
Click **Apply**.
Firewall

This section describes a firewall, which is a method designed to keep a network secure from intruders. The firewall examines traffic and filters the transmissions that do not meet the specified security criteria. The firewall decides which packets that are allowed or denied into or out of a network. This section contains the following topics:

• Basic Settings, on page 71
• Access Rules, on page 72
• Network Address Translation, on page 74
• Static NAT, on page 74
• Port Forwarding, on page 75
• Port Triggering, on page 76
• Session Timeout, on page 76
• DMZ Host, on page 77

Basic Settings

On the Basic Settings page, you can enable and configure the basic settings. You can also add trusted domains to this list. To configure the basic settings, follow these steps:

Step 1  Click Firewall > Basic Settings, and enter the following information:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall</td>
<td>Check Enable to enable the firewall settings; uncheck to disable.</td>
</tr>
<tr>
<td>DoS (Denial-of-service)</td>
<td>Check Enable to enable DoS. DoS blocks Ping of Death, SYN Flood Detect Rate [max/sec], IP Spoofing, Echo Storm, ICMP Flood, UDP Flood, and TCP Flood attacks. The traffic rate for SYN Flood, Echo Storm, ICMP Flood are configurable. The default values are: 128,15, and 100 respectively.</td>
</tr>
<tr>
<td>Block WAN Request</td>
<td>Check Enable to block the ICMP echo requests to WAN.</td>
</tr>
<tr>
<td>RESTCONF</td>
<td>By default, it is enabled on LAN interface. It can also be enabled on both LAN and WAN interfaces.</td>
</tr>
<tr>
<td>RESTCONF Port</td>
<td>By default, the port is 443 and is configurable.</td>
</tr>
<tr>
<td>NETCONF</td>
<td>By default, it is enabled on LAN interface. It can also be enabled on both LAN and WAN interfaces.</td>
</tr>
<tr>
<td><strong>NETCONF Port</strong></td>
<td>By default, port is 830 and it can be configurable.</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td><strong>LAN/VPN Web Management</strong></td>
<td>Enables the members of the LAN interface to connect to the device either through HTTP or HTTPs. Select <strong>HTTP</strong> or <strong>HTTPS</strong>.</td>
</tr>
<tr>
<td><strong>Remote Web Management</strong></td>
<td>To log remotely to the system or device and access the web interface. Check <strong>Enable</strong> to enable remote web management and enter the Port (<strong>Default 443, Range 1025-65535</strong>).</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>HTTP</strong> or <strong>HTTPS</strong>.</td>
</tr>
<tr>
<td><strong>Allowed Remote IP Address</strong></td>
<td>Check <strong>Any IP Address</strong> or enter a range of IP addresses for remote access.</td>
</tr>
<tr>
<td><strong>SIP ALG (Session Initiation Protocol Application-layer gateway)</strong></td>
<td>Check <strong>Enable</strong> to allow SIP ALG. This embeds messages of the SIP passing through a configured device with Network Address Translation (NAT) to be translated and encoded back to the packet. This application-layer gateway (ALG) is used with NAT to translate the SIP or Session Description Protocol (SDP) messages.</td>
</tr>
<tr>
<td><strong>FTP ALG Port</strong></td>
<td>Enter the port number. The default value is 21. FTP ALG port translates the FTP packets.</td>
</tr>
<tr>
<td><strong>UPnP (Universal Plug and Play)</strong></td>
<td>A set of networking protocols that permits network devices to seamlessly discover each other's presence on the network and establish functional network services for data sharing and communications. Check <strong>Enable</strong> to enable universal plug and play.</td>
</tr>
<tr>
<td><strong>Restrict Web Features</strong></td>
<td>Check to restrict the following web features:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Java</strong>: Blocks Web Java feature.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Cookies</strong>: Blocks cookies.</td>
</tr>
<tr>
<td></td>
<td>• <strong>ActiveX</strong>: Blocks ActiveX.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Access to HTTP Proxy Server</strong>: Blocks HTTP proxy servers.</td>
</tr>
<tr>
<td><strong>Exception</strong></td>
<td>Check <strong>Enable</strong> to allow only the selected web features such as Java, Cookies, ActiveX, or Access to HTTP Proxy Servers and restrict all others.</td>
</tr>
</tbody>
</table>

### Access Rules

Rules can be configured for filtering the packets based on particular parameters like IP address or ports. To configure the access rules, follow these steps:

**Step 1** Select **Firewall > Access Rules**. In the **IPv4 or IPv6 Access Rules Table**, enter the following information:

**Step 2** Click **Add** or select the row and click **Edit** and enter the following:

<table>
<thead>
<tr>
<th><strong>Rule Status</strong></th>
<th>Check <strong>Enable</strong> to enable the specific access rule. Uncheck to disable.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Action</strong></td>
<td>Choose <strong>Allows</strong> or <strong>Denies</strong> from the drop-down list.</td>
</tr>
</tbody>
</table>
| Services                  | • IPv4 – Select the service to apply IPv4 rule.  
|                          | • IPv6 – Select the service to apply IPv6 rule.  
|                          | • Services – Select the service from the drop-down list.  
| Log                      | Select True or Never from the drop-down list.  
|                          | • True – Matches the rules.  
|                          | • Never – No log required.  
| Source Interface         | Select the source interface (WAN1, WAN2, USB1, USB2, VLAN1 or Any), from the drop-down list.  
| Source Address           | Select the source IP address to which the rule is applied and enter the following:  
|                          | • Any  
|                          | • Single IP – Enter an IP address.  
|                          | • IP Range – Enter the range of IP addresses.  
|                          | • Subnet – Enter a subnet of a network.  
| Destination Interface    | Select the source interface (WAN1, WAN2, USB1, USB2, VLAN1 or Any), from the drop-down list.  
| Destination Address      | Select the source IP address to which the rule is applied and enter the following:  
|                          | • Any  
|                          | • Single IP – Enter an IP address.  
|                          | • IP Range – Enter the range of IP addresses.  
|                          | • Subnet – Enter a subnet of a network.  
| Schedule Name            | Select Business, Evening hours, Marketing, or Work from the drop-down list to apply the firewall rule. Then, click on the link to configure the schedules.  

**Step 3**
Click **Apply**.

**Step 4**
Click **Restore to Default Rules**, to restore the default rules.

**Step 5**
Click **Service Management** to configure the services.

**Step 6**
To add a service, click **Add**. To edit or delete a service, select the row and click **Edit** or **Delete**.

**Step 7**
Configure the following:

- **Application Name** – Name of the service or application.
- **Protocol** – Required protocol. Refer to the documentation for the service that you are hosting.
- **Port Start/ICMP Type/IP Protocol** – Range of port numbers reserved for this service.
- **Port End** – Last number of the port, reserved for this service.
Network Address Translation

Network address translation (NAT) enables private IP networks with unregistered IP addresses to connect to the network. NAT translates the private addresses of the internal network to public addresses before packets are forwarded to the public network.

To configure NAT, follow these steps:

---

### Step 1
Click Firewall > Network Address Translation.

### Step 2
In the NAT Table, check Enable NAT for each interface on the Interface list to enable.

### Step 3
Click Apply.

---

Static NAT

Static NAT is used to protect the LAN devices from discovery and attack. Static NAT creates a relationship that maps a valid WAN IP address to LAN IP addresses that are hidden from the WAN (Internet) by NAT.

---

### Step 1
Click Firewall > Static NAT.

### Step 2
Click Add (or select the row and click Edit) and enter the information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>Check to enable the Static NAT.</td>
</tr>
<tr>
<td>Private IP Range Begin</td>
<td>Enter the starting IP address of the internal IP address range to map to the public range.</td>
</tr>
<tr>
<td>Public IP Range Begin</td>
<td>Enter the starting IP address of the public IP address range provided by ISP.</td>
</tr>
<tr>
<td>Note</td>
<td>Do not include the device WAN IP address in this range.</td>
</tr>
<tr>
<td>Range Length</td>
<td>Enter the number of IP addresses in the range.</td>
</tr>
<tr>
<td>Note</td>
<td>The range length must not exceed the number of valid IP addresses. To map a single address, enter 1.</td>
</tr>
<tr>
<td>Services</td>
<td>Select the name of the service, from the drop-down list, to apply for the Static NAT.</td>
</tr>
<tr>
<td>Interfaces</td>
<td>Select the name of the interface from the drop-down list.</td>
</tr>
</tbody>
</table>

### Step 3
Click Service Management.

### Step 4
To add a service, click Add under the Service table. To edit or delete a service, select the row and click Edit or Delete. The fields open for modification.

### Step 5
Configure the following services:

- Application Name – Name of the service or application.
• **Protocol** – Enter the protocol.

• **Port Start/ICMP Type/IP Protocol** – Enter a range of port numbers reserved for this service.

• **Port End** – Enter the last number of the port, reserved for this service.

**Step 6** Click **Apply**.

---

**Port Forwarding**

Port forwarding allows public access to services on network devices on the LAN by opening a specific port or port range for a service, such as FTP. Port forwarding opens a port range for services such as Internet gaming that uses alternate ports to communicate between the server and the LAN host.

To configure the port forwarding, follow these steps:

**Step 1** Click **Firewall > Port Forwarding**.

**Step 2** In the **Port Forwarding Table**, click **Add** or select the row and click **Edit** and configure the following:

<table>
<thead>
<tr>
<th>Enable</th>
<th>Check to enable port forwarding.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>External Service</strong></td>
<td>Select an external service from the drop-down list. (If a service is not listed, you can add or modify the list by following the instructions in the Service Management section.)</td>
</tr>
<tr>
<td><strong>Internal Service</strong></td>
<td>Select an internal service from the drop-down list. (If a service is not listed, you can add or modify the list by following the instructions in the Service Management section.)</td>
</tr>
<tr>
<td><strong>Internal IP Address</strong></td>
<td>Enter the internal IP addresses of the server.</td>
</tr>
<tr>
<td><strong>Interfaces</strong></td>
<td>Select the interface from the drop-down list, to apply port forwarding on.</td>
</tr>
</tbody>
</table>

**Step 3** Click **Service Management**.

**Step 4** In the **Service Table**, click **Add** or select a row and click **Edit** and configure the following:

• **Application Name** – Name of the service or application.

• **Protocol** – Required protocol. Refer to the documentation for the service that you are hosting.

• **Port Start/ICMP Type/IP Protocol** – Range of port numbers reserved for this service.

• **Port End** – Last number of the port, reserved for this service.

**Step 5** Click **Apply**.

**Note** The port forwarding rules for UPnP are dynamically added by the UPnP application.

**Step 6** In the **UPnP Port Forwarding Table**, click **Refresh** to refresh the UPnP listing.
Port Triggering

Port triggering allows a specified port or port range to open for inbound traffic after user sends outbound traffic through the trigger port. Port triggering allows the device to monitor outgoing data for specific port numbers. The device recalls the client’s IP address that sent the matching data. When the requested data returns through the device, the data is sent to the proper client using the IP addressing and port mapping rules.

To add or edit a service to the port triggering table, configure the following:

Step 1  Click Add (or select the row and click Edit) and enter the information:

<table>
<thead>
<tr>
<th>Enable</th>
<th>Check to enable the port triggering rule.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Name</td>
<td>Enter the name of the application.</td>
</tr>
<tr>
<td>Trigger Service</td>
<td>Select a service from the drop-down list. (If a service is not listed, you can add or modify the list by following the instructions in the Service Management section.)</td>
</tr>
<tr>
<td>Incoming Service</td>
<td>Select a service from the drop-down list. (If a service is not listed, you can add or modify the list by following the instructions in the Service Management section.)</td>
</tr>
<tr>
<td>Interfaces</td>
<td>Select the interface from the drop-down list.</td>
</tr>
</tbody>
</table>

Step 2  Click Service Management, to add or edit an entry on the Service list.

Step 3  In the Service Table, click Add or Edit and configure the following:

- **Application Name** – Name of the service or application.
- **Protocol** – Required protocol. Refer to the documentation for the service that you are hosting.
- **Port Start/ICMP Type/IP Protocol** – Range of port numbers reserved for this service.
- **Port End** – Last number of the port, reserved for this service.

Step 4  Click Apply.

Session Timeout

With the session timeout feature, you can configure the session time-out and maximum concurrent connections for TCP/UDP/ICMP flows. The session timeout is the time it takes for the TCP or UDP session to time out after a period of idleness.

To configure the Session Timeout, follow these steps:

Step 1  Click Firewall > Session Timeout.

Step 2  Enter the following:

| TCP Session Timeout | Enter the timeout value in seconds for TCP sessions. Inactive TCP sessions are removed from the session table after this duration. |

RV340x Administration Guide
The timeout value in seconds for UDP sessions. Inactive UDP sessions are removed from the session table after this duration.

**ICMP Session Timeout**
Enter the timeout value in seconds for ICMP sessions. Inactive ICMP sessions are removed from the session table after this duration.

**Maximum Concurrent Connection**
Enter the maximum number of concurrent connections allowed.

**Current Connections**
Displays the number of current connections.

**Clear Connections**
Click to clear the current connections.

---

**DMZ Host**

DMZ is a subnetwork that is open to the public but behind the firewall. With DMZ, the packets, which enter the WAN port, can be redirected to a specific IP address on the LAN.

DMZ Host allows one host on the LAN to be exposed to the Internet to use services such as Internet gaming, video conferencing, web, or email servers. Access to the DMZ Host from the Internet can be restricted by using firewall access rules. We recommend that you place hosts that must be exposed to the WAN for services in the DMZ network.

To configure the DMZ follow these steps:

**Step 1** Choose Firewall > DMZ.

**Step 2** In DMZ Host, check Enable.

**Step 3** Enter the DMZ Host IP Address.

**Step 4** Click Apply.
This section describes a Virtual Private Network (VPN), which is used to establish an encrypted connection over a less secure network. Virtual private networks ensure secure connections to an underlying network infrastructure. A tunnel establishes a private network that can send data securely using encryption and authentication. This section contains the following topics:

- VPN Status, on page 79
- IPSec Profiles, on page 82
- Site-to-Site, on page 84
- Client to Site, on page 85
- Teleworker VPN Client, on page 88
- PPTP Server, on page 90
- L2TP Server, on page 90
- GRE Tunnel, on page 91
- SSL VPN, on page 92
- VPN Passthrough, on page 94

**VPN Status**

A Virtual Private Network (VPN) is used to establish an encrypted connection over a less secure network. VPN ensures the appropriate level of security to the connected systems when the underlying network infrastructure alone cannot provide it. A tunnel will be established a private network that can send data securely by using industry-standard encryption and authentication techniques to secure the data sent.

A remote-access VPN usually relies on either IPSec or SSL to secure the connection. VPNs provide Layer 2 access to the target network; these require a tunneling protocol such as PPTP or L2TP running across the base IPSec connection. The IPSec VPN supports site-to-site VPN for a gateway-to-gateway tunnel and client-to-server VPN for host-to-gateway tunnel. For example, a user can configure a VPN tunnel at a branch-site to connect to the device at corporate-site, so that the branch-site can securely access corporate network. The client to server VPN is useful when connecting from Laptop/PC from home to a corporate network through VPN server.

The VPN Status displays the tunnel status of the Site-to-Site, Client-to-Site, SSL VPN, PPTP, L2TP, and Teleworker VPN Client. To view the device’s VPN status, click Status > VPN Status.

**Site-to-Site Tunnel Status**

- Tunnel(s) Used – VPN tunnels in use.
- **Tunnel(s) Available** – Available VPN tunnels.
- **Tunnel(s) Enabled** – VPN tunnels enabled.
- **Tunnel(s) Defined** – Defined VPN tunnels.

In the Connection Table, you can add, edit, delete, or refresh a tunnel. (See Site-to-Site, on page 84). You can also click on **Column Display Selection** to select the column headers displayed in the Connection Table.

**Client-to-Site Tunnel Status**

In this mode, the client from Internet connects to the server to access the corporate network/LAN behind the server. For a secure connection, you can implement a client-to-site VPN. You can view all the Client-to-Tunnel connections, add, edit, or delete the connections in the Connection Table. (See Client to Site, on page 85).

The **Connection Table** displays the following:

- **Group or Tunnel Name** – Name of the VPN tunnel. This is for reference purposes only and does not match the name used at the other end of the tunnel.
- **Connections** – Status of the connection.
- **Phase2 Encryption/Auth/Group** – Phase 2 encryption type (NULL/DES/3DES/AES-128/AES-192/AES-256), authentication method (NULL/MD5/SHA1), and DH group number (1/2/5).
- **Local Group** – IP address and subnet mask of the local group.

**SSL VPN Status**

A Secure Sockets Layer virtual private network (SSLVPN) allows users to establish a secure, remote-access VPN tunnel to this device by using a web browser. SSL VPN provides secure, easy access to a broad range of web resources and web-enabled applications from almost any computer on the Internet. Here, you can view the status of the SSL VPN tunnels.

- **Tunnel(s) Used** – SSL VPN Tunnels used for connection.
- **Tunnel(s) available** – Available tunnels for the SSL VPN connection.

The **Connection Table** shows the status of the established tunnels. You can also add edit or delete connections.

- **Policy Name** – Name of the policy applied on the tunnel.
- **Session** – Number of sessions.

You can also add, edit or delete a SSL VPN. (See SSL VPN, on page 92).

**PPTP Tunnel Status**

Point-to-Point Tunneling Protocol has the capability to encrypt data with 128-bit. It is used to ensure that messages sent from one VPN node to another are secure.

- **Tunnel(s) Used** – PPTP Tunnels used for the VPN connection.
- **Tunnel(s) Available** – Available tunnels for the PPTP connection.
The **Connection Table** – shows the status of the established tunnels. You can also connect or disconnect these connections.

- **Session ID** – Session ID of the proposed or current connection.
- **Username** – Name of the connected user.
- **Remote Access** – IP address of the remotely connected or proposed connection.
- **Tunnel IP** – IP address of the tunnel.
- **Connect Time** – Time of the tunneling time.
- **Action** – Connect or disconnect the tunnel.

**L2TP Tunnel Status**

Layer 2 Tunneling Protocol is the method used to enable Point-to-Point sessions by using the Internet at Layer 2. You can find the status of L2TP Tunnel Status.

- **Tunnel(s) Used** – L2TP tunnels used for the VPN connection.
- **Tunnel(s) available** – Available tunnels for the L2TP connection.

The **Connection Table** – Shows the status of the established tunnels. You can also connect or disconnect these connections.

- **Session ID** – Session ID of the proposed or current connection.
- **Username** – Name of the connected user.
- **Remote Access** – IP address of the remotely connected or proposed connection.
- **Tunnel IP** – IP address of the tunnel.
- **Connect Time** – Time of the tunneling time.
- **Action** – Connect or disconnect the tunnel.

**Teleworker VPN Client**

You can find the status of a Teleworker VPN Client on this page. A VPN connection can be created with minimal configuration on the VPN - Teleworker VPN client page. When the Teleworker VPN client initiates the VPN connection, the IPSec VPN server pushes the IPSec policies to the Teleworker VPN client and creates the corresponding VPN tunnel.

- **Name** — Name of tunnel.
- **Status** — Current status of a tunnel whether up or down.
- **Primary DNS** — IP Address of the Primary DNS Server.
- **Secondary DNS** — IP Address of the Secondary DNS Server.
- **Primary WINS** — IP Address of primary Windows Internet Name Service (WINS).
- **Secondary DNS** — IP Address of the Secondary DNS Server.
- **Default Domain** — Name of the default domain.
• **Split Tunnel**—Name of the tunnel that allows a mobile user to access dissimilar security domains like a public network and a local LAN or WAN at the same time, VPN tunnels are enabled.

• **Split DNS**—Split DNS directs internal hosts to an internal domain name server for name resolution and external hosts are directed to an external domain name server for name resolution. Name of the split DNS.

• **Backup Server 1, 2, and 3**—When the connection to the primary IPSec VPN server fails, the security appliance can initiate the VPN connection to the backup servers. The backup server 1 has the highest priority and the backup server 3 has the lowest priority. Names of the servers defined as backup.

---

**IPSec Profiles**

The IPSec profiles contain information related to the algorithms such as encryption, authentication, and DH group for Phase I and II negotiations in auto mode. These profiles also contain keys for corresponding algorithms in case keying mode is manual. The IPSec profiles are referred in any of IPSec VPN records like site-to-site, client-to-site, or Teleworker VPN client.

To configure the IPSec Profiles, follow these steps:

**Step 1** Select VPN > IPSec Profiles.

**Step 2** Check to enable Global IPSec.

**Step 3** In the IPSec Profiles Table, click Add to add a new IPSec profile.

**Step 4** Under Add a New IPSec Profile, enter a name in the Profile Name section.

**Step 5** Select the keying mode and IKE version. The Internet Key Exchange (IKE) is a protocol that is used to set up a security association in the IPSec protocol suite. IPSec is an IP security feature that provides robust authentication and encryption of IP packets. IPsec can be configured without IKE, but IKE enhances IPsec by providing additional features, flexibility, and ease of configuration for the IPsec standard. IKE is a hybrid protocol, that implements the Oakley key exchange and Skeme key exchange inside the Internet Security Association Key Management Protocol (ISAKMP) framework. (ISAKMP, Oakley, and Skeme are security protocols implemented by IKE.)

The differences between IKEv1 and IKEv2 are as follows:

• IKEv2 does not consume as much bandwidth as IKEv1.

• IKEv2 supports EAP authentication while IKEv1 doesn’t.

• IKEv2 supports MOBIKE while IKEv1 doesn’t.

• IKEv2 has built-in NAT traversal while IKEv1 doesn’t.

• IKEv2 can detect whether a tunnel is still alive while IKEv1 cannot.

**Step 6** For Auto Keying Mode, configure the following:

**Phase 1 Options**
### Diffie-Hellman (DH) Group
Select a DH group (Group 2 or Group 5) from the drop-down list. DH is a key exchange protocol, with two groups of different prime key lengths: Group 2 has up to 1,024 bits, and Group 5 has up to 1,536 bits.

For faster speed and lower security, choose Group 2. For slower speed and higher security, choose Group 5. Group 2 is selected by default.

### Encryption
Select an encryption option (3DES, AES-128, AES-192, or AES-256) from the drop-down list. This method determines the algorithm used to encrypt or decrypt ESP/ISAKMP packets.

### Authentication
The authentication method determines how the Encapsulating Security Payload Protocol (ESP) header packets are validated. The MD5 is a one-way hashing algorithm that produces a 128-bit digest. The SHA1 is a one-way hashing algorithm that produces a 160-bit digest. The SHA1 is recommended because it is more secure. Make sure that both ends of the VPN tunnel use the same authentication method. Select an authentication (MD5, SHA1 or SHA2-256).

### SA Lifetime (Sec)
Amount of time an IKE SA is active in this phase. The default value for Phase 1 is 28,800 seconds.

---

#### Phase 2 Options

<table>
<thead>
<tr>
<th>Protocol Selection</th>
<th>Select a protocol from the drop-down list.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <strong>ESP</strong>: Select ESP for data encryption and enter the encryption.</td>
</tr>
<tr>
<td></td>
<td>• <strong>AH</strong>: Select this for data integrity in situations where data is not secret but must be authenticated.</td>
</tr>
</tbody>
</table>

| Encryption | Select an encryption option (3DES, AES-128, AES-192, or AES-256) from the drop-down list. This method determines the algorithm used to encrypt or decrypt ESP/ISAKMP packets. |

| Authentication | Select an authentication (MD5, SHA1 or SHA2-256). |

| SA Lifetime (Sec) | Amount of time a VPN tunnel (IPSec SA) is active in this phase. The default value for Phase 2 is 3600 seconds. |

<table>
<thead>
<tr>
<th>Perfect Forward Secrecy (PFS)</th>
<th>Check <strong>Enable</strong> to enable PFS and enter the lifetime in seconds, or uncheck <strong>Enable</strong> to disable.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>When the PFS is enabled, the IKE Phase 2 negotiation generates a new key for the IPSec traffic encryption and authentication. Enabling this feature is recommended.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Diffie-Hellman (DH) Group</th>
<th>Select a DH group (Group 2 or Group 5) from the drop-down list. DH is a key exchange protocol, with two groups of different prime key lengths: Group 2 has up to 1,024 bits, and Group 5 has up to 1,536 bits.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>For faster speed and lower security, choose Group 2. For slower speed and higher security, choose Group 5. Group 2 is selected by default.</td>
</tr>
</tbody>
</table>

---

**Step 7**

For **Manual Keying Mode**, configure the following:

**IPsec Configurations**
| **Security Parameter Index (SPI) Incoming** | Enter a number (Range 100 - FFFFFFFF, Default 100).  
The SPI is an identification tag added to the header while using IPsec for tunneling the IP traffic. This tag helps the kernel discern between the two traffic streams where different encryption rules and algorithms may be in use. |
| **SPI Outgoing** | Enter a number (Range 100 - FFFFFFFF, Default 100). |
| **Encryption** | Select an encryption option (**3DES, AES-128, AES-192, or AES-256**) from the drop-down list. This method determines the algorithm used to encrypt or decrypt ESP/ISAKMP packets. |
| **Key-In** | Enter a number (Hex, 48 characters). Key for decrypting ESP packets received in hex format. |
| **Key-Out** | Enter a number (Hex, 48 characters). Key for encrypting the plain packets in hex format. |
| **Authentication** | The authentication method determines how the Encapsulating Security Payload Protocol (ESP) header packets are validated. The MD5 is a one-way hashing algorithm that produces a 128-bit digest. The SHA1 is a one-way hashing algorithm that produces a 160-bit digest. The SHA1 is recommended because it is more secure. Make sure that both ends of the VPN tunnel use the same authentication method. Select an authentication (**MD5, SHA1 or SHA2-256**). |
| **Key-In** | Enter a number (Hex, 32 characters). Key for decrypting ESP packets received in hex format. |
| **Key-Out** | Enter a number (Hex, 32 characters). Key for encrypting the plain packets in hex format. |

**Step 8**  
Select an IPsec profile and click **Edit** or **Delete**.

**Step 9**  
To clone an exiting profile, select a profile and click **Clone**.

**Step 10**  
Click **Apply**.

---

**Site-to-Site**

In a site-to-site VPN, the local device at one location connects to a remote device through a VPN tunnel. Client devices can access network resources as if they were all at the same site. This model can be used for multiple users at a remote location.

A successful connection requires that at least one of the devices to be identifiable by a static IP address or a Dynamic DNS hostname. If one device has only a dynamic IP address, you can use any email address (user FQDN) or FQDN as an identification to establish the connection.

The two LAN subnets on either side of the tunnel cannot be on the same network. For example, if the Site A LAN uses the 192.168.1.x/24 subnet, Site B can use 192.168.2.x/24.

To configure a tunnel, enter corresponding settings (reversing local and remote) when configuring the two devices. Assume that this device is identified as device A. Enter its settings in the Local Group Setup section; enter the settings for the other device (device B) in the Remote Group Setup section. When you configure the other device (device B), enter its settings in the Local Group Setup section, and enter the device A settings in the Remote Group Setup section.

To configure the Site-to-Site VPN, follow these steps:
Step 1: Click VPN > Site-to-Site.

Step 2: In the Site to Site table, the following will be displayed:

<table>
<thead>
<tr>
<th><strong>Connection Name</strong></th>
<th>The name of the VPN tunnel connection created using VPN Setup Wizard. It does not have to match the name used at the other end of the tunnel.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Remote Endpoint</strong></td>
<td>IP Address of the remote endpoint to where the VPN connection is intended. This can be an FQDN or an IP address.</td>
</tr>
<tr>
<td><strong>Interface</strong></td>
<td>Interface used for the tunnel.</td>
</tr>
<tr>
<td><strong>IPSec Profile</strong></td>
<td>IPSec profile used for the VPN tunnel.</td>
</tr>
<tr>
<td><strong>Local Traffic Selection</strong></td>
<td>Traffic selectors from which traffic is originating.</td>
</tr>
<tr>
<td><strong>Remote Traffic Selection</strong></td>
<td>Traffic selectors to which traffic is destined.</td>
</tr>
<tr>
<td><strong>Status</strong></td>
<td>Status of the tunnel.</td>
</tr>
</tbody>
</table>
| **Actions**         | • **Edit** – Click to edit the connection, it navigates to Site to Site - Add or Edit a New Connection page.  
                     • **Delete** – Click to delete the connection.  
                     • **Connect** – Click to connect and establish the tunnel.  
                     • **Disconnect** – Click to disconnect the connection. |

---

**Client to Site**

Clients from the Internet can connect to the server to access the corporate network or a LAN behind the server. This feature creates a new VPN tunnel to allow teleworkers and business travelers to access your network by using third-party VPN client software.

To open the Client-to-Site page, click VPN > Client-to-Site and the follow will be displayed:

<table>
<thead>
<tr>
<th><strong>Tunnel Name</strong></th>
<th>Name of the connected tunnel.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WAN Interface</strong></td>
<td>Name of the interface with which the groups are connected.</td>
</tr>
<tr>
<td><strong>Authentication Method</strong></td>
<td>Name of the authentication method through which they are connected.</td>
</tr>
</tbody>
</table>

**Adding a Client-to-Site Connection**

Step 1: Click Add and, select an option (Cisco VPN Client or 3rd Party Client).

Step 2: For Cisco VPN Client, configure the following:

<table>
<thead>
<tr>
<th><strong>Enable</strong></th>
<th>Click Enable to enable the configuration.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tunnel Name</strong></td>
<td>Enter a name for the tunnel.</td>
</tr>
<tr>
<td>Interface</td>
<td>Select the interface (WAN1, WAN2, USB1, or USB2) from the drop-down list.</td>
</tr>
<tr>
<td>IKE Authentication Method</td>
<td>Authentication method to be used in IKE negotiations in IKE-based tunnels.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Pre-shared Key</strong>: IKE peers authenticate each other by computing and sending a keyed hash of data that includes the Pre-shared Key. If the receiving peer is able to create the same hash independently using its Pre-shared key, it knows that both peers must share the same secret, thus authenticating the other peer. Pre-shared keys do not scale well because each IPSec peer must be configured with the Pre-shared key of every other peer with which it establishes a session. Enter the Pre-shared Key, and click <strong>Enable</strong> to enable the Minimum Pre-shared Key Complexity. To display the Pre-shared key, check <strong>Enable</strong> in the Show Pre-shared key section.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Certificate</strong>: The digital certificate is a package that contains information such as a certificate bearer's identity: name or IP address, the certificate's serial number, the certificate's expiration date, and a copy of the certificate bearer's public key. The standard digital certificate format is defined in the X.509 specification. X.509 version 3 defines the data structure for certificates. Select the certificate from the drop-down list.</td>
</tr>
<tr>
<td>User Group</td>
<td>Click <strong>Add</strong> to add a user group. (Click <strong>Delete</strong> to delete a user group.</td>
</tr>
<tr>
<td>Mode</td>
<td>Select the mode from the options.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Client</strong>: Client request for IP address and server supplies the IP addresses from the configured address range. Select <strong>Client</strong> and enter the start and end IP addresses for client’s LAN.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Network Extension Mode (NEM)</strong>: Clients propose their subnet for which VPN services need to be applied on traffic between LAN behind server and subnet proposed by client.</td>
</tr>
<tr>
<td>Pool Range for Client LAN</td>
<td><strong>Start IP</strong> – Enter the start IP address for the pool range. <strong>End IP</strong> - Enter the end IP address for the pool range.</td>
</tr>
<tr>
<td>For Mode Configuration</td>
<td></td>
</tr>
<tr>
<td>Primary DNS</td>
<td>Enter the IP address of the primary DNS server.</td>
</tr>
<tr>
<td>Secondary DNS</td>
<td>Enter the IP address of the secondary DNS server.</td>
</tr>
<tr>
<td>Primary Windows Internet Name Service (WINS) Server</td>
<td>Enter the IP address of the primary WINS.</td>
</tr>
<tr>
<td>Secondary WINS Server</td>
<td>Enter the IP address of the secondary WINS.</td>
</tr>
<tr>
<td>Default Domain</td>
<td>Enter the name of the default domain to be used in remote network.</td>
</tr>
<tr>
<td>Back Server 1, 2, &amp; 3</td>
<td>Enter the IP address or domain name of the back servers 1, 2 and 3. When the connection to the primary IPSec VPN server fails, the security appliance can start the VPN connection to the backup servers. The backup server 1 has the highest priority and the backup server 3 has the lowest priority.</td>
</tr>
<tr>
<td>Split Tunnel</td>
<td>Check to enable split tunnel. Then click <strong>Add</strong>, to enter an IP address and netmask for the split tunnel. You can add, edit, or delete a split tunnel.</td>
</tr>
</tbody>
</table>
### Split DNS
Check **Enable** to enable the Split DNS. Then click **Add**, to enter an domain name for the split DNS. You can add, edit, or delete a split tunnel.

### For a 3rd Party Client

#### Step 3
In the Basic Settings tab, configure the following:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable</strong></td>
<td>Click <strong>Enable</strong> to enable the configuration.</td>
</tr>
<tr>
<td><strong>Tunnel Name</strong></td>
<td>Name of the VPN tunnel. This description is for your reference. It does not have to match the name used at the other end of the tunnel.</td>
</tr>
<tr>
<td><strong>Interface</strong></td>
<td>Select the interface (WAN1, WAN2, USB1, or USB2) from the drop-down list.</td>
</tr>
<tr>
<td><strong>IKE Authentication Method</strong></td>
<td>Authentication method to be used in IKE negotiations in IKE-based tunnels.</td>
</tr>
<tr>
<td>• <strong>Pre-shared Key</strong></td>
<td>IKE peers authenticate each other by computing and sending a keyed hash of data that includes the Pre-shared key. If the receiving peer is able to create the same hash independently using its Pre-shared key, it knows that both peers must share the same secret, thus authenticating the other peer. Pre-shared keys do not scale well because each IPSec peer must be configured with the Pre-shared key of every other peer with which it establishes a session. Enter the Pre-shared Key, and click Enable to enable the Minimum Pre-shared Key Complexity.</td>
</tr>
<tr>
<td>• <strong>Certificate</strong></td>
<td>The digital certificate is a package that contains information such as a certificate bearer's identity: name or IP address, the certificate's serial number, the certificate's expiration date, and a copy of the certificate bearer's public key. The standard digital certificate format is defined in the X.509 specification. X.509 version 3 defines the data structure for certificates. Select the certificate from the drop-down list.</td>
</tr>
<tr>
<td><strong>Local Identifier</strong></td>
<td>Select the local identifier type (IP Address, FQDN, or User FQDN) from the drop-down list and enter the identifier.</td>
</tr>
<tr>
<td><strong>Remote Identifier</strong></td>
<td>Select the remote identifier (Remote IP, FQDN, or User FQDN) from the drop-down list and enter the identifier.</td>
</tr>
<tr>
<td><strong>Extended Authentication</strong></td>
<td>Check <strong>Extended Authentication</strong> to enable. Click <strong>Add</strong> to add an extended authentication and select admin or guest.</td>
</tr>
<tr>
<td><strong>Pool Range for Client LAN</strong></td>
<td><strong>Start IP</strong> - Enter the start IP address for the pool range. <strong>End IP</strong> - Enter the end IP address for the pool range.</td>
</tr>
</tbody>
</table>

#### Step 4
In the Advanced Settings tab, configure the following:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IPSec Profile</strong></td>
<td>Name of the IPSec profile to be used for the VPN tunnel. Set to Default.</td>
</tr>
<tr>
<td><strong>Remote Endpoint</strong></td>
<td>Select the remote endpoint (Static IP, FQDN, or Dynamic IP) from the drop-down list.</td>
</tr>
</tbody>
</table>

**For Local Group Setup**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Local IP Type</strong></td>
<td>Select the local IP type (IP address or Subnet) from the drop-down list.</td>
</tr>
</tbody>
</table>

**For Mode Configuration**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Primary DNS</strong></td>
<td>Enter the IP address of the primary DNS server.</td>
</tr>
</tbody>
</table>
### Secondary DNS
Enter the IP address of the secondary DNS server.

### Primary Windows Internet Name Service (WINS) Server
Enter the IP address of the primary WINS.

### Secondary WINS Server
Enter the IP address of the secondary WINS.

### Default Domain
Enter the name of the default domain to be used in remote network.

### Split Tunnel
Check to enable split tunnel. Then click **Add**, to enter an IP address and netmask for the split tunnel. You can add, edit, or delete a split tunnel.

### Split DNS
Check to enable split DNS. Then click **Add**, to enter an domain name for the split DNS. You can add, edit, or delete a split tunnel.

### Additional Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggressive Mode</td>
<td>Check <strong>Aggressive Mode</strong> to enable. The Aggressive Mode feature allows you to specify RADIUS tunnel attributes for an IP security (IPsec) peer and to initiate an Internet Key Exchange (IKE) aggressive mode negotiation with the tunnel attributes.</td>
</tr>
<tr>
<td>Compress (Support IP Payload compression Protocol (IP Comp))</td>
<td>Check <strong>Compress</strong> to enable the device to propose compression when it starts a connection. If the responder rejects this proposal, then the device does not implement compression. When the device is the responder, it accepts compression, even if compression is not enabled. If you enable this feature for this device, also enable it on the device at the other end of the tunnel.</td>
</tr>
</tbody>
</table>

### Step 5
Click **Apply**.

---

### Teleworker VPN Client

The Teleworker VPN Client feature minimizes the configuration requirements at remote locations by allowing the device to work as a Cisco VPN hardware client. When the Teleworker VPN Client starts the VPN connection, the IPSec VPN server pushes the IPSec policies to the Teleworker VPN Client and creates the corresponding tunnel.

To configure the Teleworker VPN Client, follow these steps:

### Step 1
Click **VPN > Teleworker VPN Client** to see the following:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Teleworker VPN Client</td>
<td>Select <strong>On</strong> or <strong>Off</strong> to switch on or off the Teleworker VPN Client.</td>
</tr>
<tr>
<td>Auto Initiation Retry</td>
<td>Select <strong>On</strong> or <strong>Off</strong> to retry for auto initiation to establish the connection.</td>
</tr>
<tr>
<td>Retry Interval</td>
<td>Time to re-establish the tunnel after failure. Enter the time in seconds. The maximum time is 1800 seconds.</td>
</tr>
</tbody>
</table>
Step 2

In the Teleworkers VPN Client table, click **Add** and provide the following information:

### Basic Settings

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a name for the profile.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server (Remote Address)</td>
<td>Enter the remote server's IP address.</td>
</tr>
<tr>
<td>Active Connection on Startup</td>
<td>To start connection on startup. At any point, only one profile can be in On state to start negotiations at startup</td>
</tr>
</tbody>
</table>

#### IKE Authentication Method

Authentication method to be used in IKE negotiations in IKE-based tunnels.

- **Pre-shared Key**: IKE peers authenticate each other by computing and sending a keyed hash of data that includes the Pre-shared Key. If the receiving peer is able to create the same hash independently using its Pre-shared key, it knows that both peers must share the same secret, thus authenticating the other peer. Pre-shared keys do not scale well because each IPSec peer must be configured with the Pre-shared key of every other peer with which it establishes a session. Check **Pre-shared Key**, and enter a group name and password in the designated fields.

- **Certificate**: The digital certificate is a package that contains information such as a certificate bearer's identity: name or IP address, the certificate's serial number, the certificate's expiration date, and a copy of the certificate bearer's public key. The standard digital certificate format is defined in the X.509 specification. The X.509 version 3 defines the data structure for certificates. Check **Certificate** and select **Default**.

<table>
<thead>
<tr>
<th>Mode</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>— Client request for IP address and server supplies the IP addresses from the configured address range. Select <strong>Client</strong> and enter the username and password.</td>
</tr>
<tr>
<td>Network Extension Mode (NEM)</td>
<td>— Clients propose their subnet for which VPN services need to be applied on traffic between LAN behind server and subnet proposed by client. The ezvpn client NEM mode only supports LAN IP 10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16. Also, the LAN behind the server and client should be in a different subnet when in NEM mode. Select <strong>NEM</strong> and select VLANs from the drop-downs and enter the username and password.</td>
</tr>
</tbody>
</table>

### Advanced Settings

<table>
<thead>
<tr>
<th>Backup Server 1, 2 and 3</th>
<th>Enter the IP address or domain name of the back servers 1, 2 and 3.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>When the connection to the primary IPSec VPN server fails, the security appliance can start the VPN connection to the backup servers. The backup server 1 has the highest priority and the backup server 3 has the lowest priority.</td>
</tr>
<tr>
<td>Peer Timeout</td>
<td>Enter the time in seconds (Range 30 to 480).</td>
</tr>
</tbody>
</table>

Step 3

Click **Apply**.
PPTP Server

The Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks. PPTP uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets. Up to 25 PPTP (Point-to-Point Tunneling Protocol) VPN tunnels can be enabled for users who are running PPTP client software. In the Wizard, the user selects the option to create a connection to the workplace by using a VPN connection.

To configure the PPTP Server, follow these steps.

**Step 1**
Click **VPN > PPTP Server**, and provide the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PPTP Server</strong></td>
<td>Select <strong>On</strong> or <strong>OFF</strong> to enable or disable PPTP server.</td>
</tr>
<tr>
<td><strong>Start and End IP Address</strong></td>
<td>If PPTP has been enabled, enter start and end IP addresses.</td>
</tr>
<tr>
<td><strong>DNS1 and 2 IP Addresses</strong></td>
<td>Enter the IP address of the primary and secondary DNS server.</td>
</tr>
<tr>
<td><strong>User Authentication</strong></td>
<td>Select the user authentication (<strong>Admin</strong> or <strong>Default</strong>).</td>
</tr>
<tr>
<td><strong>Microsoft Point-to-Point (MPPE) Encryption</strong></td>
<td>The MPPE encrypts data in PPP-based dial-up connections or PPTP VPN connections. 128-bit key MPPE encryption schemes are supported. Select the MPPE encryption (<strong>None or 128 bits</strong>) from the drop-down list.</td>
</tr>
</tbody>
</table>

**Step 2**
Click **Apply**.

**Note** The PPTP Server currently only supports PAP as local database authentication method. In order to support Microsoft Point-to-Point (MPPE) Encryption with MS-CHAPv2, it will require an external authentication server.

L2TP Server

Layer Two Tunneling Protocol (L2TP) is an extension of the PPTP used by an Internet service provider (ISP) to enable VPN over the Internet. L2TP does not provide encryption for the data it tunnels. Instead, they rely on other security protocols, such as IPsec, to encrypt their data.

The L2TP tunnel is established between the L2TP Access Concentrator (LAC) and the L2TP Network Server (LNS). An IPsec tunnel is also established between these devices and all L2TP tunnel traffic is encrypted using IPsec.

To configure the L2TP Server, follow these steps:

**Step 1**
Click **VPN > L2TP Server**.

**Step 2**
Provide the following information:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>L2TP Server</strong></td>
<td>Check <strong>On</strong> or <strong>Off</strong> to enable or disable the L2TP server.</td>
</tr>
</tbody>
</table>
Maximum Transmission Unit | The size of the largest packet that can be sent over L2TP tunnel. If L2TP has been enabled, enter the size of a packet (Range 128-1400, Default 1400).
---|---
Address Pool | • Start IP Address — Enter the start IP address.  
• End IP Address — Enter the end IP address.
---|---
DNS1 and 2 IP Addresses | Enter the primary and secondary IP addresses of the DNS1 and 2 servers.
---|---
User Authentication | Select the user authentication (Group Name or admin).
---|---
IPSec | Check On to enable IPSec security for the L2TP tunnel.
---|---
IPSec Profile | Default
---|---
Pre-shared Key | Enter the Pre-shared Key to use to authenticate the remote IKE peer. You can enter up to 30 keyboard characters or hexadecimal values, such as My_@123 or 4d795f40313233. Both ends of the VPN tunnel must use the same Pre-shared Key. We recommend that you change the Pre-shared Key periodically to maximize VPN security.
---|---
Show Pre-shared Key | Check Enable to display the pre-shared key.
---|---

**Step 3**  
Click Apply.

---

**GRE Tunnel**

Generic Routing Encapsulation (GRE) is one of the available tunneling mechanisms which uses an IP as the transport protocol and carries many different passenger protocols. The tunnels behave as virtual point-to-point links that have two endpoints identified by the tunnel source and tunnel destination addresses at each endpoint.

**Step 1**  
Click VPN > GRE Tunnel. Then, click Add to add a new GRE tunnel and provide the following:

<table>
<thead>
<tr>
<th>GRE Tunnel Name</th>
<th>Select the name of the GRE tunnel from the drop-down list.</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRE Tunnel Description</td>
<td>Enter a description for the GRE tunnel.</td>
</tr>
<tr>
<td>Enable</td>
<td>Check to enable the GRE tunnel.</td>
</tr>
<tr>
<td>Source</td>
<td>Select the tunnel source from the drop-down list.</td>
</tr>
<tr>
<td>Destination</td>
<td>Select the tunnel destination from the drop-down list.</td>
</tr>
<tr>
<td>IP Address of GRE tunnel</td>
<td>Enter the IP address of the tunnel which carries the transport protocol.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Enter the subnet mask of the GRE tunnel.</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum Transmission Unit (MTU) is the size of the largest packet that can be sent over the network. The default setting is 1400 bytes, which is the standard value for Ethernet networks.</td>
</tr>
</tbody>
</table>

**Step 2**  
Click Apply.
SSL VPN

The Secure Sockets Layer Virtual Private Network (SSLVPN) allows users to remotely access restricted networks, using a secure and authenticated pathway by encrypting the network traffic. The device supports Cisco AnyConnect VPN client which can be downloaded at [http://www.cisco.com/go/anyconnect/]. The device supports 2 SSL VPN tunnels by default, and the user can register a license to support up to 50 tunnels. Once installed and activated, the SSL VPN will establish a secure, remote-access VPN tunnel.

In addition, a Cisco AnyConnect Secure Mobility Client license is required to install and use the Cisco AnyConnect Secure Mobility Client on your device. Information on how to order the Cisco AnyConnect Secure Mobility User Licenses can be found here [http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf]. We do recommend the AnyConnect Plus License for 25-99 users.

To configure the SSL VPN, follow these steps:

**Step 1**
Click VPN>SSL VPN.

**Step 2**
On the General Configuration Server tab, provide the following information:

**Mandatory Gateway Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco SSL VPN Server</td>
<td>Select On or Off to enable or disable the server.</td>
</tr>
<tr>
<td>Gateway Interface</td>
<td>Select the gateway interface (WAN1, WAN2, USB1 or USB2) from the drop-down list.</td>
</tr>
<tr>
<td>Gateway Port</td>
<td>Enter the port number of the gateway (Range 1 to 65535).</td>
</tr>
<tr>
<td>Certificate File</td>
<td>Default.</td>
</tr>
<tr>
<td>Client Address Pool</td>
<td>Enter the IP address of the client address pool.</td>
</tr>
<tr>
<td>Client Netmask</td>
<td>Enter the client netmask.</td>
</tr>
<tr>
<td>Client Domain</td>
<td>Enter the client domain name.</td>
</tr>
<tr>
<td>Login Banner</td>
<td>Enter the text to appear as login banner.</td>
</tr>
</tbody>
</table>

**Optional Gateway Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Idle Timeout</td>
<td>Enter the idle timeout in seconds (Range 60 to 86,400).</td>
</tr>
<tr>
<td>Session Timeout</td>
<td>Time it takes for the TCP or UDP session to time out after a period of idleness. Enter the session timeout in seconds (Range 60 to 1,209,600).</td>
</tr>
<tr>
<td>Client DPD Timeout</td>
<td>Sends periodic HELLO/ACK messages to check the status of the VPN tunnel. This feature must be enabled on both ends of the VPN tunnel. Specify the interval between HELLO/ACK messages in the Interval field. Enter the client DPD timeout in seconds (Range 0 to 3600).</td>
</tr>
</tbody>
</table>
**Gateway DPD Timeout**
Sends periodic HELLO/ACK messages to check the status of the VPN tunnel. This feature must be enabled on both ends of the VPN tunnel. Specify the interval between HELLO/ACK messages in the Interval field. Enter the gateway DPD timeout in seconds (Range 0 to 3600).

**Keep Alive**
Ensures that your device is always connected to the Internet. Attempts to re-establish the VPN connection if it is dropped. Enter the Keep Alive time in seconds (Range 0 to 600).

**Lease Duration**
Enter the time in seconds during the tunnel to be connected (Range 600 to 1,209,600).

**Max MTU**
Enter the size in bytes of a packet that can be sent over the network (Range 576 to 1406).

**Rekey Interval**
Enter the rekey interval time in seconds (Range 0 to 43,200).

**Step 3**
Click **Apply**.

**Step 4**
On the Group Policies tab, click **Add** and provide the following information to configure the SSLVPN group policy.

**Basic Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Policy Name</strong></td>
<td>Enter the policy name. Group policies that apply whole sets of attributes to a group of users, rather than having to specify each attribute individually for each user.</td>
</tr>
<tr>
<td><strong>Primary DNS</strong></td>
<td>Enter the IP address of the primary DNS server.</td>
</tr>
<tr>
<td><strong>Secondary DNS</strong></td>
<td>Enter the IP address of the secondary DNS server.</td>
</tr>
<tr>
<td><strong>Primary WINS</strong></td>
<td>Enter the IP address of the primary WINS.</td>
</tr>
<tr>
<td><strong>Secondary WINS</strong></td>
<td>Enter the IP address of the secondary WINS.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Enter a description for the SSLVPN policy.</td>
</tr>
</tbody>
</table>

**IE Proxy Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IE Proxy Policy</strong></td>
<td>Internet Explorer proxy settings to establish VPN tunnel. Select the IE Proxy Policy (None, Auto, Bypass-Local, or Disabled) from the drop-down list.</td>
</tr>
</tbody>
</table>

If you select **Auto** or **Bypass-Local** enter the following:

- **Address** — IP address or domain name.
- **Port** — Enter a port number (Range 1 to 65,535).

**Step 5**
In the IE Exception Proxy Table, click **Add**, **Edit** or **Delete** to add, edit or delete IE exceptions.

**Split Tunneling Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable Split Tunneling</strong></td>
<td>Check Enable Split Tunneling to allow Internet destined traffic to be sent unencrypted directly to the Internet. Full Tunneling sends all traffic to the end device where it is then routed to destination resources (eliminating the corporate network from the path for web access).</td>
</tr>
<tr>
<td><strong>Split Selection</strong></td>
<td>Select Include Traffic to include traffic or Exclude Traffic when applying the split tunneling.</td>
</tr>
</tbody>
</table>

**Step 6**
In the Split Network Table, click **Add**, **Edit** or **Delete** to add, edit or delete split DNS exceptions.
Step 7 Configure the IP and Netmask.
Step 8 Click **Apply**.

---

**VPN Passthrough**

The VPN Passthrough allows VPN clients to pass through this device and connect to a VPN endpoint. It is enabled by default.

To configure the VPN Passthrough, follow these steps:

---

**Step 1** Select **VPN > VPN Passthrough**.

**Step 2** To enable VPN Passthrough, check **Enable** for each of the approved protocols:

- **IPSec Passthrough** – Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer.

- **PPTP Passthrough** – Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network.

- **L2TP Passthrough** – Layer 2 Tunneling Protocol is the method used to enable Point-to-Point sessions by using the Internet at Layer 2.

**Step 3** Click **Apply**.

---
CHAPTER 11

Security

This section describes the network security, which consists of the policies adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and contains the following topics:

• Application Control, on page 95
• Web Filtering, on page 97
• Content Filtering, on page 98
• IP Source Guard, on page 99
• Cisco Umbrella, on page 99
• Threat/IPS, on page 100

Application Control

Application Control is an additional security feature on the router that can enhance a secured network, promote productivity in the workplace, and maximize bandwidth. Application control can be useful for smartphones and other browser-based applications.

Settings

To add, configure, or modify the application control policies, follow these steps:

Step 1 Click Security > Application Control > Settings.
Step 2 Check On or Off to activate the application control.
Step 3 To create a new application control policy, click Add.
Step 4 On the Policy Profile-Add/Edit section, specify the following information:

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>Enter a name for the policy profile.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Enter a short description about the policy.</td>
</tr>
<tr>
<td>Enable</td>
<td>Check to enforce the application control policy.</td>
</tr>
<tr>
<td>Application</td>
<td>Click Edit and select the content to be filtered (blocked or logged etc) from the list and click Apply.</td>
</tr>
<tr>
<td>IP Groups</td>
<td>Select an IP Group from the drop-down list to apply the policy.</td>
</tr>
</tbody>
</table>
Select a device type from the drop-down list.

Select the OS type from the drop-down list.

Under Exclusion List Table, click Add and configure the following:

- **Type** (Select Mac or IP Group)
- **IP/MAC** – Enter MAC address
- **Device Type** – Select device type
- **OS Type** – Select OS type

To specify when the Application Control policy should be active, select the schedule from the drop-down list to apply web filtering.

**Step 5** Click Apply.

### Application Statistics

To open the Application Statistics page, click **Security > Application Control > Application Statistics**. The following will be displayed:

<table>
<thead>
<tr>
<th>Current WAN traffic update</th>
<th>Select the time duration (15/30/60) in seconds to see the traffic on the selected WAN interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong></td>
<td>This is applicable for WAN Ethernet's interfaces only.</td>
</tr>
<tr>
<td><strong>WAN Interface</strong></td>
<td>Select the interface to see the statistics presented in a graphical format.</td>
</tr>
</tbody>
</table>

In the Application Statistics section, click the refresh button to refresh the statistics.

**Applications**

<table>
<thead>
<tr>
<th>Application</th>
<th>Displays the name of the application. Click on the link to see the list of clients using it.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Protocol of the application traffic such as TCP/UDP/Other.</td>
</tr>
<tr>
<td>Port</td>
<td>Application's port (destination port) of traffic.</td>
</tr>
<tr>
<td>% Usage</td>
<td>Usage percentage of total applications.</td>
</tr>
<tr>
<td>Usage</td>
<td>Application in usage listed according to size.</td>
</tr>
<tr>
<td>Sent</td>
<td>Packets sent out.</td>
</tr>
<tr>
<td>Received</td>
<td>Packets received.</td>
</tr>
<tr>
<td>#Clients</td>
<td>Number of clients using this application.</td>
</tr>
</tbody>
</table>
Client Statistics

The Client Statistics display the historical data of clients that are or have been connected to the device. To view the Client Statistics page, click **Security > Application Control > Client Statistics**. On the Client Statistics page, any existing groups with associated clients will be displayed in the Client Groups Table. You can add a group or edit an existing group by either click **Add** and enter a group name or selecting a group and click **Edit**.

To view and edit the client details, provide the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>Displays client's MAC address. Click to see all associated applications.</td>
</tr>
<tr>
<td>IPv4 or IPv6 Address</td>
<td>Displays the client's IP address.</td>
</tr>
<tr>
<td>Status</td>
<td>Current status of the client.</td>
</tr>
<tr>
<td>Hostname</td>
<td>Hostname of the client. Click to edit the hostname.</td>
</tr>
<tr>
<td>Device Type</td>
<td>Device name of client. Click to edit.</td>
</tr>
<tr>
<td>OS Type</td>
<td>Displays OS type of the client. Click to edit.</td>
</tr>
<tr>
<td>Usage %</td>
<td>Usage percentage of total clients.</td>
</tr>
<tr>
<td>IP Group</td>
<td>Displays the IP group associated. Select the appropriate IP group.</td>
</tr>
</tbody>
</table>

Web Filtering

Web filtering is a feature that allows you to manage access to inappropriate websites. It can screen a client’s web access requests to determine whether to allow or deny that website. To enable and configure web filtering, follow these steps:

**Step 1** Click **Security > Web Filtering**.
**Step 2** On the Web Filtering section, select **On or Off** and click **Apply**.
**Step 3** Enter the URL in the URL lookup, to verify or lookup a URL. You can view the category, reputation score and status of that URL. If you want to modify the URL Categorization/Score, follow the URL Ratings Review links.
**Step 4** In the Web Filtering Policies table, click **Add**. To edit an existing policy and click **Edit** to modify it.
**Step 5** On the Web Filtering — Add/Edit Policy page, enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Name</td>
<td>Specify a name for the web filtering policy you are creating.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a short description for the policy.</td>
</tr>
<tr>
<td>Enable</td>
<td>Check <strong>Enable</strong> to activate the policy.</td>
</tr>
</tbody>
</table>
Content Filtering

Content filtering enables you to restrict access to clients from certain designated unwanted websites. It can block access to websites based on the domain names and keywords. It is also possible to schedule when the content filtering should be active.

To configure and enable content filtering, follow these steps:

Step 1  Click Security > Content Filtering.
Step 2  Check Enable Content Filtering to enable.
Select the desired radio button.

Step 3

<table>
<thead>
<tr>
<th>Block Matching URLs</th>
<th>Check Block Matching URLs to block specific domains and keywords.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Only Matching URLs</td>
<td>Check Allow Only Matching URLs to allow only the specified domains and keywords.</td>
</tr>
</tbody>
</table>

Step 4
Under Filter by Domain table, click Add.

Step 5
Enter a domain you want to filter/allow in the Domain Name column.

Step 6
To specify when the content filtering rules are active, select the schedule from the Schedule drop down list.

Step 7
Under Filter by Keyword, click Add.

Step 8
Enter the keywords to be blocked/allowed in the Keyword Name column.

Step 9
To specify when the content filtering rules are active, select the schedule from the Schedule drop down list. You can modify an existing domain name or keyword name by selecting the same and clicking Edit.

Step 10
Click Apply.

---

**IP Source Guard**

The IP Source Guard is a security feature that restricts IP traffic on untrusted IPs and MAC addresses by filtering traffic based on the configured IP MAC bindings. It is a filter that permits traffic on LAN ports only when the IP address and MAC address of each packet matches entries in the IP-MAC Binding table. This feature helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

To configure the IP source guard, follow these steps:

Step 1
Click Security > IP Source Guard.

Step 2
Check Enable IP Source Guard if IP and MAC binding are required.

Step 3
Check Block Unknown MAC Address, if only the MAC address requires filtering irrespective of the IP Address.

Step 4
In the IP & MAC Binding Table, click Add and enter the Static IPv4 address and MAC address for binding.

Step 5
Click Add to the IP and MAC Binding Table in the DHCP Lease Table to add these entries to the IP & MAC Binding Table.

Step 6
Specify a name for this binding table entry under the Name column.

Step 7
Click Apply, Edit or Delete to apply a new address, or to edit or delete an existing address.

---

**Cisco Umbrella**

Cisco Umbrella is a cloud security platform that provides a first line of defense against threats on the Internet. This feature provides cloud-based security service by inspecting the DNS query which is sent to the DNS server. Using an Umbrella account, the integration will transparently intercept DNS queries and redirect them to Umbrella. This device will appear in the Umbrella dashboard as a network device for applying policy and viewing report.

To configure the Umbrella, follow these steps:
Step 1  Click Security > Cisco Umbrella.
Step 2  Check Enable to enable the Umbrella feature.
Step 3  Check Block LAN DNS query to block the LAN DNS query.
Step 4  If you select to use the Network Device as the device's identity, (preferred, if available in your Umbrella subscription) follow these steps:

<table>
<thead>
<tr>
<th>Getting Started</th>
<th>Click to enter the following credentials:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Enter the Key and Secret, which were copied from the Umbrella account and click Next.</td>
</tr>
<tr>
<td></td>
<td>2. Select your organization and click Next.</td>
</tr>
<tr>
<td></td>
<td>3. Select the required policies to be associated and click Next.</td>
</tr>
<tr>
<td></td>
<td>4. Enter a name of the device. A success message will appear if the registration is successful. Next, click OK.</td>
</tr>
</tbody>
</table>

Step 5  If you use Network as this device's identity, check this option.
Step 6  Next, add your router's public IP address to the Umbrella dashboard. Or, if you have a dynamic public IP address, you can manually add it on to the Umbrella dashboard or follow the instructions here.
Step 7  Configure the appropriate policies on the Cisco Umbrella portal to either allow or deny traffic towards the fully qualified domain name (FQDN).
Step 8  The device is now registered. Next, complete the following tasks if required:
Step 9  To configure the Advanced Configuration settings complete the following:

<table>
<thead>
<tr>
<th>Local Domain to Bypass</th>
<th>Enter the local domain names to be bypassed from the OpenDNS resolver.</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNSCrypt</td>
<td>• DNSCrypt is always enabled on this Network Device Configuration option.</td>
</tr>
<tr>
<td></td>
<td>Provide the Public Key of the OpenDNS resolver to update the resolver list.</td>
</tr>
</tbody>
</table>

Threat/IPS

The dashboard displays the details of the threats and attacks when the Anti Threat and IPS features are configured. The dashboard gives you a view of the entire events summary, and detailed information of threats and attacks detected as per selection such as day, week, and month.

Status

The dashboard displays the details of the threats and attacks when the Anti Threat and IPS features are configured. The dashboard gives you a view of the entire events summary, and detailed information of threats and attacks detected as per selection such as day, week, and month.
Click **Security > Threat/IPS > Status**. You can see the system date and time, scanned, and detected threats and attacks of the selected tab. By default, you can see the Total tab's status.

<table>
<thead>
<tr>
<th>Total</th>
<th>Select Last 24 hours, Week, or Month from the list to display the events.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat</td>
<td>Displays the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Top 10 clients</strong> - the list of mac addresses who are affected.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Top 10 threats</strong> - the list of threats detected.</td>
</tr>
<tr>
<td>IPS</td>
<td>Displays the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Top 10 Attacked Clients</strong> - the list of top 10 attacked clients</td>
</tr>
<tr>
<td></td>
<td>• <strong>Top 10 IPS Attacks</strong> - the list of the top 10 IPS attacks</td>
</tr>
</tbody>
</table>

## Antivirus

The Antivirus protects the network users from infected and malware content received in emails or data. The Antivirus feature supports SMTP, HTTP, FTP, POP3 and IMAP protocols.

Configure the appropriate settings on the Antivirus page for protection against malware or infected emails.

To configure the Antivirus feature, follow these steps:

**Step 1** Click **Security > Threat/IPS > Antivirus**.

**Step 2** Check **Enable**, if you want to enable this feature.

**Step 3** Configure the following options in the Applications to Scan frame.

<table>
<thead>
<tr>
<th>HTTP/FTP/SMTP/POP3/IMAP</th>
<th>• Check <strong>Enable</strong> to activate the configuration.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Select the appropriate action.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Log</strong> - Select this option to generate the log only (with client information, signature ID, etc.) when the threats are identified. It does not impact the connection.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Log Destroy</strong> - Select this option to drop the connection when the threats are identified and logs the message for deletion.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> In the case of an identified threat in an attachment, it will truncate the file during the download process.</td>
</tr>
</tbody>
</table>

| Enable File Size Threshold | Select the check box and enter the required file size to scan. |

**Virus Database**
IPS

Intrusion Prevention System (IPS) inspects the network for traffic anomalies. You can configure the IPS to block or log of he configured security level.

To configure the IPS, follow these steps:

**Step 1**
Click **Security > IPS**.

**Step 2**
Select **On** to enable the Intrusion Prevention System feature.

| Mode               | Block Attacks (Prevention) - select to block all the attacks. It also logs the anomaly.  
|--------------------|------------------------------------------------------------------  
|                    | Log Only - select this option to generate the log only (with client information, signature ID, etc.) when the anomalies are identified. It does not impact the connection.  
| IPS Security Level | Connectivity - select to apply the selected mode on the traffic to detect the most critical attacks. This provides the least protection: only (high severity) risk attacks are detected.  
|                    | Balanced - select to apply the selected mode on the traffic to detect the severe attacks along with the critical attacks. This provides medium protection: (High + medium severity) are inspected, bypassing low risk signatures.  
|                    | Security - select to apply the selected mode on the traffic to detect the normal attacks along with the severe and critical attacks. This provides the most protection: All rules (high + medium + low severity) are inspected.  

**Intrusion Prevention System Signatures**

| Last Update | Displays the date and time of the last updated signature.  
| File Version | Displays the signature version which is being used.  
|-------------|-----------------------------------------------------
### Search by IPS Signature ID
Enter the Signature's ID and click to check whether the signature is supported or not.

### IPS Signature Table

<table>
<thead>
<tr>
<th>Name, ID, Severity, and Category</th>
<th>Use First, Previous, Next, and Last buttons to display the signatures from the given number and set the order of display. Also, from the Lines Per Page drop-down list, select the number of signatures to display.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name of the signature.</strong></td>
<td>• Name of the signature.</td>
</tr>
<tr>
<td><strong>The unique identifier of the signature.</strong></td>
<td>• The unique identifier of the signature. To view the complete details for the selected signature, click on the link in the column.</td>
</tr>
<tr>
<td><strong>Severity level denotes the security impact.</strong></td>
<td>• Severity level denotes the security impact.</td>
</tr>
<tr>
<td><strong>The category that the signature belongs to.</strong></td>
<td>• The category that the signature belongs to.</td>
</tr>
</tbody>
</table>
CHAPTER 12

QoS

This section describes the Quality of service (QoS), which is used to optimize network traffic in order to improve the user experience. QoS controls and manages network resources by setting priorities for specific types of data (video, audio, files) on the network. It is exclusively applied to network traffic generated for video on demand, IPTV, VoIP, streaming media, videoconferencing, and on-line gaming. This section contains the following topics:

• Traffic Classes, on page 105
• WAN Queuing, on page 106
• WAN Policing, on page 107
• WAN Bandwidth Management, on page 107
• Switch Classification, on page 107
• Switch Queuing, on page 108

Traffic Classes

Traffic classes channel Internet traffic to a desired queue based on the service. The service can be Layer 4 TCP or UDP port application, Source or Destination IP Address, DSCP, Receive interface, OS, and Device type.

To configure the Traffic Classes, follow these steps:

Step 1
Click QoS > Traffic Classes.

Step 2
In the Traffic Table, click Add (or select the row and click Edit) and enter the following:

• Class Name – Enter the name of the defined class.
• Description – Enter the description of the class.
• In Use – Traffic class record is being used by a queuing policy.

Step 3
In the Service Table, click Add (or select the row and click Edit) and enter the following information:

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Enter the name of the service.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receive Interface</td>
<td>Select an interface (WAN1, WAN2, USB1, USB2, LAN1, LAN2, LAN3, LAN4, or VLAN1) from the drop-down list.</td>
</tr>
</tbody>
</table>
**IP Version** | Select **IPv4, IPv6, or Either** (if you do not know the version of the traffic).
---|---
**Source IP** | Enter the source IP address of the traffic.
**Destination IP** | Enter the destination IP address of the traffic.
**Service/Application** | • **Service**: Select the name of the service to apply on the traffic record. Provide the source and destination ports.
• **Application**: Select the application to apply on the traffic record. Select the application behavior and category.
**Note** | The Application rules can not be configured until the user enables the Application Control in the Security/Application Control page.
**Device Type** | Select the type of device from the drop-down list, from which the traffic is initiated.
**OS Type** | Select the Operating System of the device from the drop-down list, from which the traffic is initiated.
**Match DSCP** | The DSCP matches the traffic class value in the IPv6 header for the IPv6 traffic. The traffic class value is 4 times the configured value. For example, if the user configures the matched DSCP as 10, then rewrite the DSCP as 18. The rule matches the IPv6 flows with the traffic class value 40 and rewrites the DSCP to 72. Select the DSCP value from the drop-down list, to be matched with the DSCP value in the incoming packets.
**Rewrite DSCP** | Select the DSCP value from the drop-down list, to be replaced with, in incoming packets.

**Step 4**  
Click **Apply**.

---

**WAN Queuing**

Net traffic coming from the LAN-to-WAN can be managed in three modes (Rate Control, Priority, and Low Latency) which are mutually exclusive.

To configure WAN Queuing, follow these steps:

**Step 1**  
Click **QoS > WAN Queuing**.

**Step 2**  
Above the WAN Queuing Table, select the desired Queuing Engine (**Priority**, **Rate-control**, or **Low-latency**).

**Step 3**  
In the WAN Queuing Table, click **Add** and enter a name for the policy and provide a description.

**Step 4**  
If Priority Queuing was selected, in the Queuing Priority Table, select the Traffic Class for each queue from the drop-down list.

**Step 5**  
If Rate Control Queuing was selected, in the Queuing Rate-Control Table, select the Traffic Class and enter the Minimum and Maximum Rate for each queue.

**Step 6**  
If Low-latency Queuing was selected, in the Queuing Low-Latency Table, select the Traffic Class and configure the bandwidth share value for each queue.

**Step 7**  
Click **Apply**.
WAN Policing

In WAN Policing, the rate-control mode supports eight queues. Each queue can be configured with a maximum rate.

To configure the WAN Policing page, follow these steps:

Step 1  Click QoS > WAN Policing.
Step 2  Check Enable policing of traffic on WAN interfaces.
Step 3  In the Policy Class Table, configure the following for each queue:

<table>
<thead>
<tr>
<th>Traffic class</th>
<th>Select Unspecified or Default.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Rate</td>
<td>Enter the queue’s maximum rate of bandwidth in percentages to limit the incoming traffic from WAN to LAN.</td>
</tr>
</tbody>
</table>

Step 4  Click Apply.

WAN Bandwidth Management

WAN interfaces can be configured with the maximum bandwidth provided by the ISP. When the value (transfer rate in KBP/S) is configured, the traffic entering the interface is shaped in defined rate.

To configure the WAN Bandwidth Management, follow these steps:

Step 1  Click QoS > WAN Bandwidth Management.
Step 2  In the WAN Bandwidth Management Table, select the Interface and configure the following:

<table>
<thead>
<tr>
<th>Upstream (kb/s)</th>
<th>Enter the upstream traffic rate in kb/s.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Downstream (kb/s)</td>
<td>Enter the downstream traffic rate in kb/s. *You will need to enable WAN policing for Downstream Bandwidth, otherwise the downstream bandwidth will not take effect.</td>
</tr>
<tr>
<td>Outbound Queuing Policy</td>
<td>Select the outbound queuing policy to be applied to the WAN interface.</td>
</tr>
</tbody>
</table>

Step 3  Click Apply.

Switch Classification

In QoS modes such as Port-based, DSCP-based, and CoS-based, packets are sent out.

To configure Switch Classification, click QoS > Switch Classification and follow these steps:
Step 1

Select the desired Switch QoS Mode (Port-based, DSCP-based or CoS-based).

| Port-based | The incoming packets on each LAN port which are mapped to specific queues, based on the mappings.  
• LAN Port Queue — Select the LAN Port Queue to map the traffic coming on the individual LAN ports.  
• LAG Port Queue — When LAG is enabled, all traffic entering this LAG interface is mapped using a configured queue. |
| --- | --- |
| DSCP-based | For IPv6 traffic, the DSCP matches the traffic class value in the IPv6 header and places it in different queues. The traffic class value is 4 times the DSCP value. For example, if the user configures the DSCP as 10 mapping to Queue 1, then the IPv6 flows with traffic class value 40 will be put into Queue 1. The switch must use the DSCP field of the incoming packets and schedule the packet for prioritization into a particular queue using the mapping table.  
• Based on the DSCP value of the incoming packet, map the traffic to the different queues.  
Click Restore Defaults to restore the default values. |
| CoS-based | The switch uses the incoming packet priority 'CoS; bits and classifies the packet to user configured queue.  
• Based on the CoS value of the incoming packet, map the traffic to the different queues by selecting the queues from the drop-down list. |

Step 2

Click Apply.

Switch Queuing

In Switch Queuing, the queue weight for all the four queues per port can be configured by assigning weights to each queue. The range of weights can be from 1 to 100. When LAG is enabled, the user can define the queue weights for all four queues.

Note

If the weight is 0, this means that the queue is in highest priority queue.

To configure LAN Port Queue Weight, click QoS > Switch Queuing and complete the following steps:

Step 1
In LAN Port Queue Weight table, enter the appropriate weight for each of the queues.

Step 2
Click Apply.

Step 3
Click Restore Defaults to restore system default settings.
Step 4  
In the LAG Port Queue Weight table, the LAG ports and their queue weights are displayed.
Chapter 13

Configuration Wizards

This section describes how to configure the device and contains the following topics:

- Initial Setup Wizard, on page 111
- Application Control Wizard, on page 111
- VPN Setup Wizard, on page 112

Initial Setup Wizard

The Initial Setup Wizard will guide you in configuring your device for Internet access.

1. Click on Configuration Wizards from the device's graphical user interface.
2. Next, click Launch Wizard to setup the device and follow the on-screen instructions. The Initial Setup Wizard tries to automatically detect and configure your connection. If it cannot, the Initial Setup Wizard may ask you for information about your Internet connection. You may need to contact your ISP to obtain this information.
3. After the Initial Setup Wizard is done configuring the device, you are required to change the default password. Change the default password and continue completing the instructions on the screen.
4. Log in to the device with the new username and password. The device getting started page appears. It displays the most common configuration tasks.
5. Click one of the tasks listed in the navigation bar to complete the configuration. For detailed instructions on each of the sections listed on the device manager, visit the applicable chapter or section in the administration guide.

Application Control Wizard

Application Control is an additional security feature on the device that can enhance an already secured network, promote productivity in the workplace, and maximize bandwidth. Application control can be useful for smartphones and other browser-based applications.

The application control is configured globally, but is not used by a policy unless you apply an action to a policy. After you create an Application Control action in the Application Control configuration, you can change the Application Control action to enable it for each policy.

To add, configure, or modify the application control policies, follow these steps:
VPN Setup Wizard

A VPN allows a remote host to act as if they were located on the same local network. The device supports 50 tunnels. The VPN Setup Wizard guides in configuring a secure connection for site-to-site IPSec tunnel. This simplifies the configuration by avoiding complex and optional parameters, so any user can set up the IPSec tunnel in a fast and efficient manner.

To start the VPN Setup Wizard, click Configuration Wizards > VPN Setup Wizard. The wizard can be used to create a Site to Site VPN tunnel. Follow the steps below to create a VPN tunnel.

**Step 1**
In the Getting Started section, enter a connection name in the **Give this connection a name** box.

**Step 2**
Select an interface (WAN1, WAN2, USB1, or USB2) from the drop-down list.

**Step 3**
Click Next.

**Step 4**
In the Remote Router Settings section, select the **Remote Connection Type** from the drop-down list. If you select **IP Address**, enter the IP Address, or if you select a fully qualified domain name (FQDN), enter the name.

**Step 5**
Click Next, to move to the next screen.

**Step 6**
In the Local and Remote Networks section, under Local Traffic Selection, select the Local IP (IP Address or Subnet) from the drop-down list. If you select **IP Address**, enter the IP address, or if you select **Subnet**, enter the IP address and subnet mask.

**Step 7**
Under Remote Traffic Selection, select the Remote IP (IP Address or Subnet) from the drop-down list. If you select **IP Address**, enter the IP address or if you select **Subnet**, then enter the IP address and subnet mask.

**Step 8**
Click Next.

**Step 9**
In the IPSec Profile, select the IPSec profile from the drop-down list.

**Step 10**
If you select **Default**, then click Next.

**Step 11**
If you select **New Profile**, configure the following:

**Phase 1 Options**

| **Diffie-Hellman (DH) Group** | Select a DH group (**Group 2 or Group 5**) from the drop-down list. DH is a key exchange protocol, with two groups of different prime key lengths: Group 2 has up to 1,024 bits, and Group 5 has up to 1,536 bits. For faster speed and lower security, choose Group 2. For slower speed and higher security, choose Group 5. Group 2 is selected by default. |

VPN Setup Wizard
### Encryption
Select an encryption option (3DES, AES-128, AES-192, or AES-256) from the drop-down list. This method determines the algorithm used to encrypt or decrypt ESP/ISAKMP packets.

### Authentication
The authentication method determines how the Encapsulating Security Payload Protocol (ESP) header packets are validated. The MD5 is a one-way hashing algorithm that produces a 128-bit digest. The SHA1 is a one-way hashing algorithm that produces a 160-bit digest. The SHA1 is recommended because it is more secure. Make sure that both ends of the VPN tunnel use the same authentication method. Select an authentication (MD5, SHA1 or SHA2-256).

<table>
<thead>
<tr>
<th>SA Lifetime (Sec)</th>
<th>Amount of time an IKE SA is active in this phase. The default value for Phase 1 is 28,800 seconds.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perfect Forward Secrecy (PFS)</td>
<td>Check Enable to enable PFS and enter the lifetime in seconds, or uncheck Enable to disable. When the PFS is enabled, the IKE Phase 2 negotiation generates a new key for the IPSec traffic encryption and authentication. Enabling this feature is recommended.</td>
</tr>
<tr>
<td>Pre-Shared Key</td>
<td>Pre-shared key to use to authenticate the remote IKE peer. You can enter up to 30 keyboard characters or hexadecimal values, such as My_@123 or 4d795f40313233. Both ends of the VPN tunnel must use the same Pre-shared Key. We recommend that you change the Pre-shared Key periodically to maximize VPN security.</td>
</tr>
</tbody>
</table>

### Phase 2 Options

<table>
<thead>
<tr>
<th>Diffie-Hellman (DH) Group</th>
<th>Select a DH group (Group 2 or Group 5) from the drop-down list. DH is a key exchange protocol, with two groups of different prime key lengths: Group 2 has up to 1,024 bits, and Group 5 has up to 1,536 bits. For faster speed and lower security, choose Group 2. For slower speed and higher security, choose Group 5. Group 2 is selected by default. Note This is enabled only when Perfect Forward secrecy is enabled under Phase 1 Options.</th>
</tr>
</thead>
</table>
| Protocol Selection | Select a protocol from the drop-down list. 
  - ESP: Select ESP for data encryption and enter the encryption. 
  - AH: Select this for data integrity in situations where data is not secret but must be authenticated. |
| Encryption | Select an encryption option (3DES, AES-128, AES-192, or AES-256) from the drop-down list. This method determines the algorithm used to encrypt or decrypt ESP/ISAKMP packets. |
| Authentication | Select an authentication (MD5, SHA1 or SHA2-256). |
| SA Lifetime (Sec) | Amount of time a VPN tunnel (IPSec SA) is active in this phase. The default value for Phase 2 is 3600 seconds. |

**Step 12** Click **Next** to see the summary of all configurations.
Step 13  
Click Submit.
License

The Cisco Smart Licensing is a cloud-based approach to licensing. It simplifies the licensing experience by rendering it easier to purchase, deploy, track and renew Cisco software. When you start the device for the first time, you will be in evaluation mode. Your Cisco product must be registered and managed through Cisco Smart Licensing. To register and manage your new Cisco product, click Smart Licensing Manager and register for a Cisco Smart account if you don't have one.

To access the License page, select License > License.

A pop-up will appear stating that your URL is not whitelisted and you are not registered to allow access. You must register your Cisco Product with the Cisco Smart Software Licensing. To register your product, follow these steps:

- Ensure that the product has access to the internet.
- Log in to your Smart Account in Smart Licensing Manager.
- Navigate to the Virtual Account containing the licenses to be used in this product instance.
- Generate a Product Instance Registration Token (this identifies your Smart Account) and copy or save it.
- Click Register and paste the Token into the window that appears.

In the License section, you can configure the licenses or register the device. It simplifies the Cisco software experience and helps you understand how the Cisco software is used.
Request a Smart Account

A Smart Account provides a repository for Smart enabled Cisco devices and enables Users to manage their Cisco licenses. Users can activate and monitor their license usage as well as track any future Cisco purchases. You will need to create a Customer Smart Account to fully utilize the license management features of the device.

To request a Customer Smart Account, log into Cisco Software Central (CSC). If you do not have a CCO ID, go to www.cisco.com and click Register now.

Step 1 Access Cisco Software Central.
Step 2 Go to Administration and then click on Request Smart Account.
Step 3 Select "Yes, I have the authority to represent my company" and you will authorize the Smart Account activation. Select "No, the person specified below should be notified to authorize activation" if you do not have the authority or prefer not to authorize the Smart Account.
Step 4 Next, enter the account name and click Continue.
   Optional — Edit the account domain identifier if needed by following these steps:
Step 5 In the Edit Account Identifier, change the Domain Identifier by editing the domain or adding a prefix.
Step 6 Click OK to confirm the new domain ID.
Step 7 Verify the account name and edit if required.
Step 8 Click Continue to proceed with the Smart Account request.
   Note If you edit the Account Domain Identifier at the time of the Smart Account request, Cisco will contact you to complete the approval process.

Step 9 Optional — Enter company information. If you selected the option No under account authorization, you must provide the company name and address by completing the required fields.
Step 10 Optional — Nominate users for administrative access by entering the email ID of the users you select for administrative access.
Step 11 Verify the Smart Account information and the users who requested administrative access. Next, click Submit Request. After submitting the Smart Account request, you will receive a confirmation message that account request has been completed. The request is pending until it is authorized by the specified person.
   Note A provisional Smart account will be created after submitting the request. Orders can be assigned to a provisional Smart Account but items purchased cannot be used until the Smart Account is activated.

Smart Software Licensing Status

The Smart Software Licensing Status section displays your device’s license information.

Registration Status — Registered or Unregistered, and date of registration.

License Authorization Status — Authorized or Evaluation Mode or Out of Compliance or Authorization Expired or Evaluation Period Expired and the date of license authorization.
Export-Controlled Functionality — Not allowed by default.

Smart License Usage

You can select the Smart License to be used for the device. Make sure that you have enough of licenses in the virtual account for the device, otherwise it is not compliant.

To configure the Smart License, follow these steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Under Smart License Usage, click Choose Licenses.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Check the applicable license.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Save.</td>
</tr>
<tr>
<td>Step 4</td>
<td>A License Authorization Renewal pop-up will appear, click OK.</td>
</tr>
</tbody>
</table>
CHAPTER 15

Where To Go From Here

This section contains the following topics:
- Where To Go From Here, on page 119

**Where To Go From Here**

**Support**

<table>
<thead>
<tr>
<th>Service</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Open Source Requests</td>
<td>Select a link to download the firmware for your Cisco product. No login is required.</td>
</tr>
</tbody>
</table>

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.