User Guide for Cisco Configuration Professional for Catalyst 2960-L Smart Managed Switches, Release 15.2(7)E

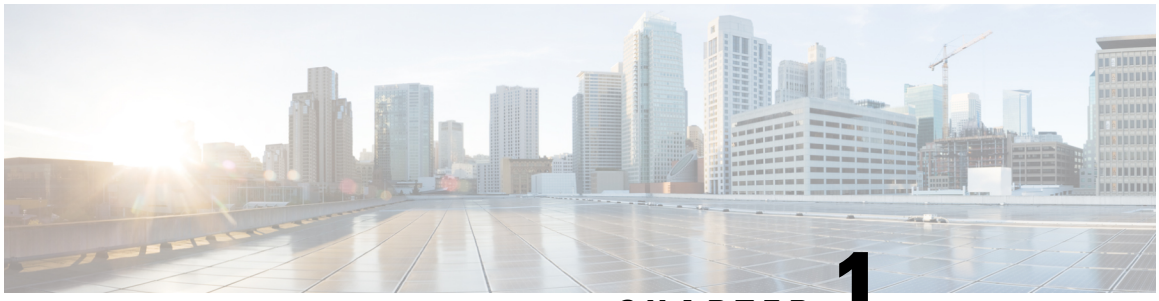
First Published: 2019-04-24

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

PART I

Web User Interface Elements



CHAPTER 1

Using the Web UI

Using the Web UI

The Web user interface (Web UI) provides network administrators with a single solution for monitoring, and optimizing the Cisco Catalyst 2960-L Smart Managed Switches.

System Requirements

You can access the application from a client web browser. Ensure that the following web client requirements are met:

- Hardware - A Mac (OS version 10.9.5) or Windows (OS version 7) laptop or desktop compatible with one of the following tested and supported browsers:
  - Google Chrome 52 or later
  - Mozilla Firefox 48 or later
  - Apple Safari 9 or later
  - Microsoft Internet Explorer 11, or later
- Display resolution - We recommend that you set the screen resolution to 1280 x 800 or higher.

Using the Toolbar

The application pages contain the following static global toolbar at the top right corner:

- Language—Click to select the language of your choice. By default, it is the preferred language configured in your browser settings. The supported languages are English, Espanol, Deutsche, Korean, Chinese and Japanese.
- Help—Launches the online help for the Web user interface. If you get a page blocked message on the address bar, allow the page to be displayed by allowing pop-ups for the site.
- System Information—Displays information such as the device name and the image on your device.

- Alerts—Displays latest/unseen alerts. Click the alerts icon, to see all the alerts that are currently reported by your device. The severity 1 alerts are displayed in red. The alerts are reported at intervals of one minute.
- Save Configuration—Saves your configuration.
- Telnet—Allows you to run supported CLI commands from within the Web UI.
- Renew Certificate—Allows you to renew certificate.
- Logout—Allows you to terminate an active session.

Using the Navigation Menu

The Web user interface allows you to perform the following tasks from the navigation pane:

- **Monitoring** - Monitor your network on a daily basis and perform other ad-hoc operations related to network device inventory and configuration management. View the dashboard for a snapshot of connected client devices, performance information, incidents, and search options.
- **Configuring** - Configure access to the switch's general configuration, management interface configuration, STP, VLAN and Bluetooth configuration. Run basic tests and diagnostics to assess the health of the switch.
- **Services** - Access and configure Routing (Static, RIP), Energy Saver and Security services.
- **General Settings** - Specify system configuration settings and user administration settings.
- **Help** - Access help content for the Web UI.

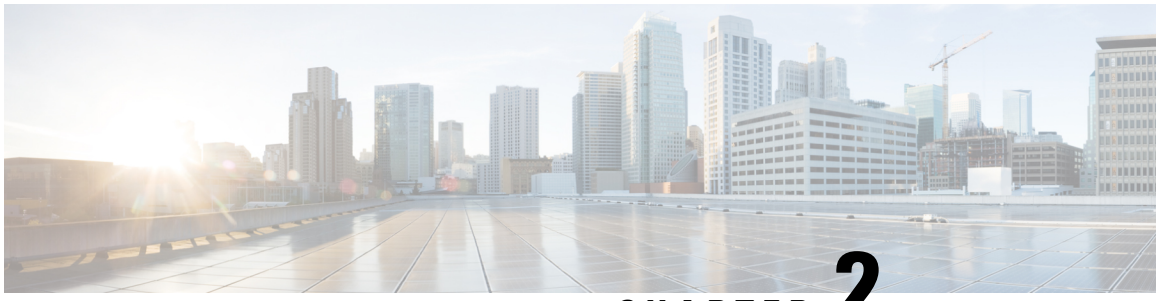
Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

You can also subscribe to the *What's New in Cisco Product Documentation* RSS feed, which delivers lists and content of new and revised Cisco technical documentation directly to your desktop, using any RSS reader application. This RSS feed is a free service.

PART II

Quick Setup Tasks



CHAPTER 2

Quick Setup Tasks on Your Device

Getting Started with Device Configuration

On the first day with your new device, you can perform a number of tasks to ensure that your device is online, reachable and easily configured. These configurations are applicable for all the supported switches and ME based Access Points.

Quick Setup: Accessing the Configuration Setup Wizard

When you first set up the switch, use the Configuration Setup wizard to enter the initial IP information. This enables the switch to connect to local routers and the Internet. You can then access the switch through the IP address for further configuration.

1		Mode button
2		SYST LED (system)
3		STAT LED (status)
4		SPEED LED
5		PoE LED [1]
6		Console LED
7		Port LEDs

[1] Only on switch models that support PoE.

Before you Begin: If your PC has a static IP address, change your PC settings to temporarily use DHCP.

Step 1 If you want to configure wireless controller and APs, connect them now to the switch. Verify that no devices are connected to the switch. Initially, the switch acts as a DHCP server.

Step 2 Confirm that the STAT LED is solid green. This indicates that POST is complete. If the STAT LED turns amber, the device failed POST. Reconnect the AC power cord to the AC power connector of your device and to a grounded AC outlet. If the STAT LED still does not turn green, contact your Cisco representative or retailer.

Step 3 Connect a straight-through Category 5 Ethernet cable to a 10/100/1000 Ethernet port on the switch front panel and to the Ethernet port on the PC.

Step 4 Verify that the port LEDs on the PC and on your device are solid green or blinking green. This indicates a successful connection.

Step 5 Wait for a minute until the switch assigns an IP address to the PC.

Step 6 To log on to the device, type the IP address https://192.168.1.1 in the address bar of your Web browser on your PC and press Enter.

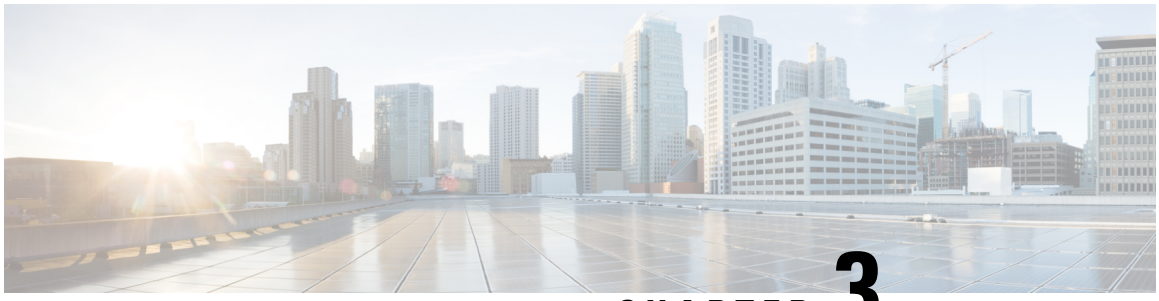
Step 7 Type the following default credentials: username (**smartm**) and password (**c2960lsm**) and click **OK**.

It is recommended to create a new username and password after the first login and delete the default credentials.

Continue configuration the device using the Cisco Configuration Professional for Catalyst.

PART III

Monitoring



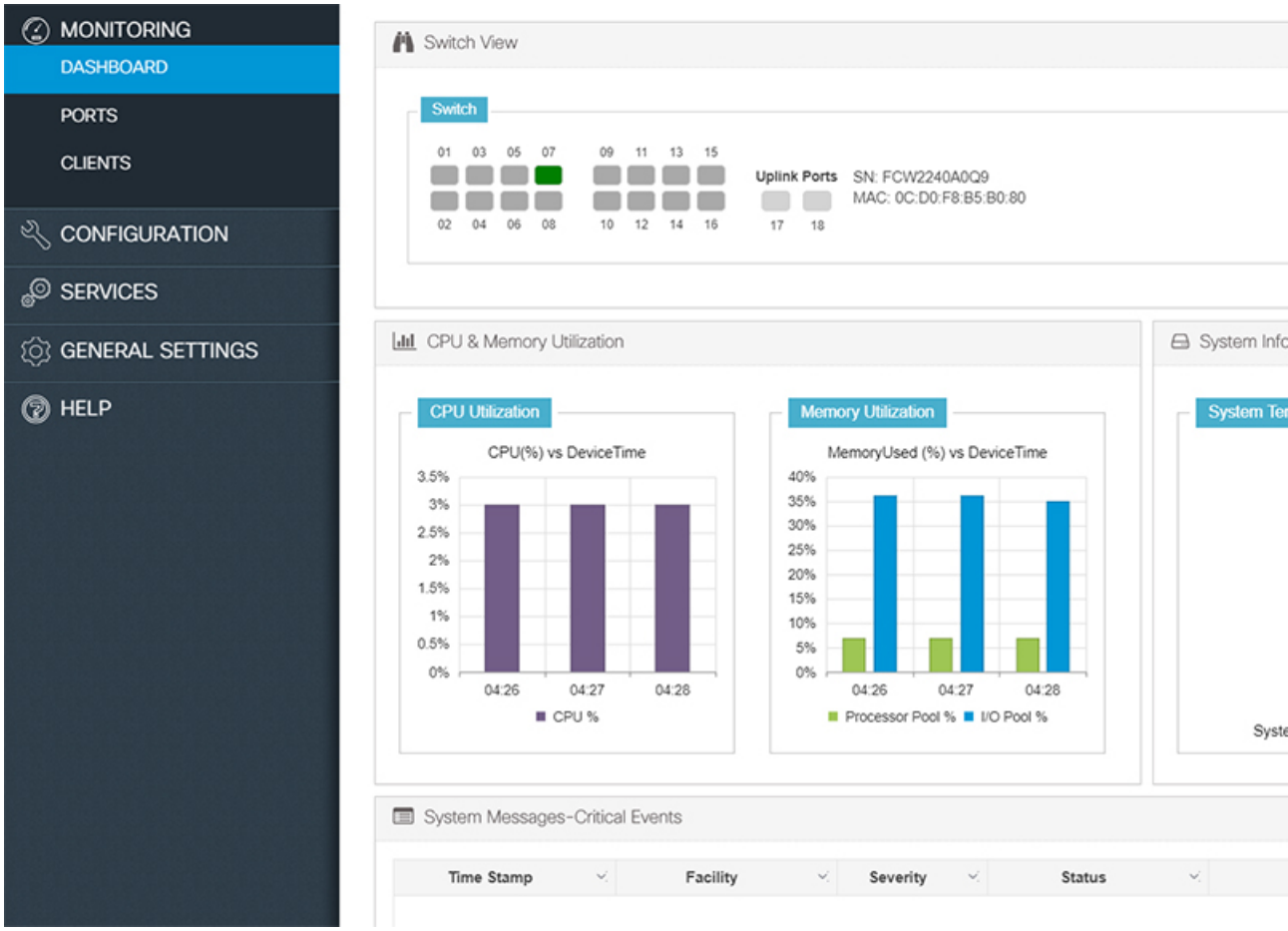
CHAPTER 3

Monitoring the Device

Understanding the Dashboard

The **Monitoring > Dashboard** page displays a snapshot of the overall status and statistics for your device.

Figure 1: Dashboard

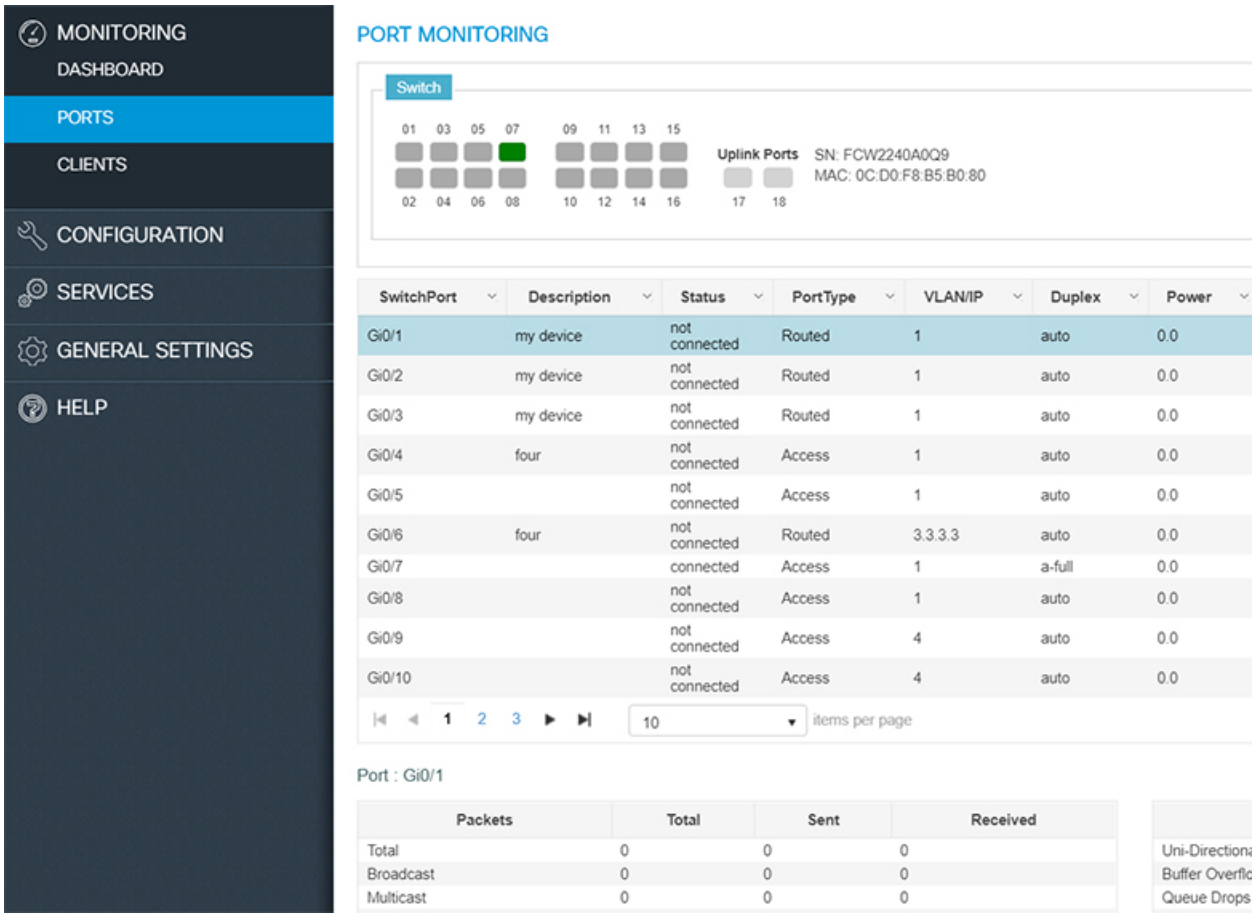


- **Switch View** - Displays a snapshot of the ports on the device.
- **CPU and Memory Utilization** - Displays CPU usage on the processors on each core, every 5 minutes, every 1 minute and every 5 seconds. The Memory Utilization section displays a chart of the device memory usage. Hover over the graph to view the processor pool and the I/O pool percentage.
- **System Information** - The **PoE Power Consumption** section displays a pie-chart showing the total Power over Ethernet (PoE), Universal Power over Ethernet (UPoE) on the device, the power used by the device and the current power available. The **System Temperature** section displays the temperature of the device. If the temperature is yellow or red, your device needs attention.
- **System Messages-Critical Events** - Displays high severity, critical alerts that require your attention. Displays the system messages or any critical events regarding the switch in a tabular format that can also be downloaded using the **Export** button.

Monitoring Ports

The **Monitoring > Ports > Port Monitoring** page enables you to track and monitor the port parameters (interface details) like type of interface, description, port status, port type of the switch. The logical representation of the ports at the top provides an easy-to-understand snapshot of all ports on the device.

Figure 2: Port Monitoring



You can get additional details associated with the port by clicking on the port in the logical view at the top or in the table.

Parameter	Description
Switch Port	The type of interface. • Gigabit Ethernet—Displays the Gigabit Ethernet for 10/100/1000 Mb/s Ethernet ports. • 10 Gigabit Ethernet—Displays the 10-Gigabit Ethernet for 10,000 Mb/s Ethernet ports. • SFP—Displays the small form-factor pluggable (SFP) module Gigabit Ethernet interfaces. • Unknown—Displays unknown when no interface is configured. • SVI port • Port-channel
Description	The description associated with the port.
Status	The connection status of the port.
Port Type	The type of port—Access, Trunk, Routed.
VLAN/IP	The VLAN connection link associated with the port. Values are as follows: • Trunk Mode—Displays the VLAN ID of the VLAN associated with this port. • Access Mode—Displays the VLAN ID of the VLAN associated with this port.
Duplex	The duplex mode of the interface.
Power	The power (in Watts) of the interface.
Speed	The speed of the interface.
PktDrop	Number of dropped packets.
SwitchType	Displays the type of Switch—Standalone.

Monitoring Clients

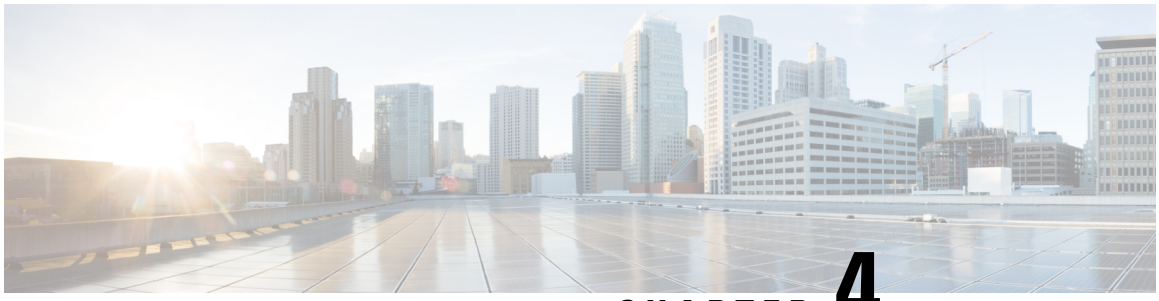
The **Monitor > Clients** page lists the information about the clients connected to the device. Click the client in the table to view properties and statistics for each client.

Parameter	Description
MAC	The MAC address of the client.
Switch Port	The interface used for communication between the client and the switch.
Client Name	Name of the client.
OS	Software version of the client.

Parameter	Description
Manufacturer	Client manufacturer details.
IP	IP address of the client.
VLAN	The VLAN on which the client resides.
POE Drawn	Determines power drawn(wattage) by this client.
Images	An icon to help you identify the device.

PART IV

Configuration



CHAPTER 4

Configuring the Device

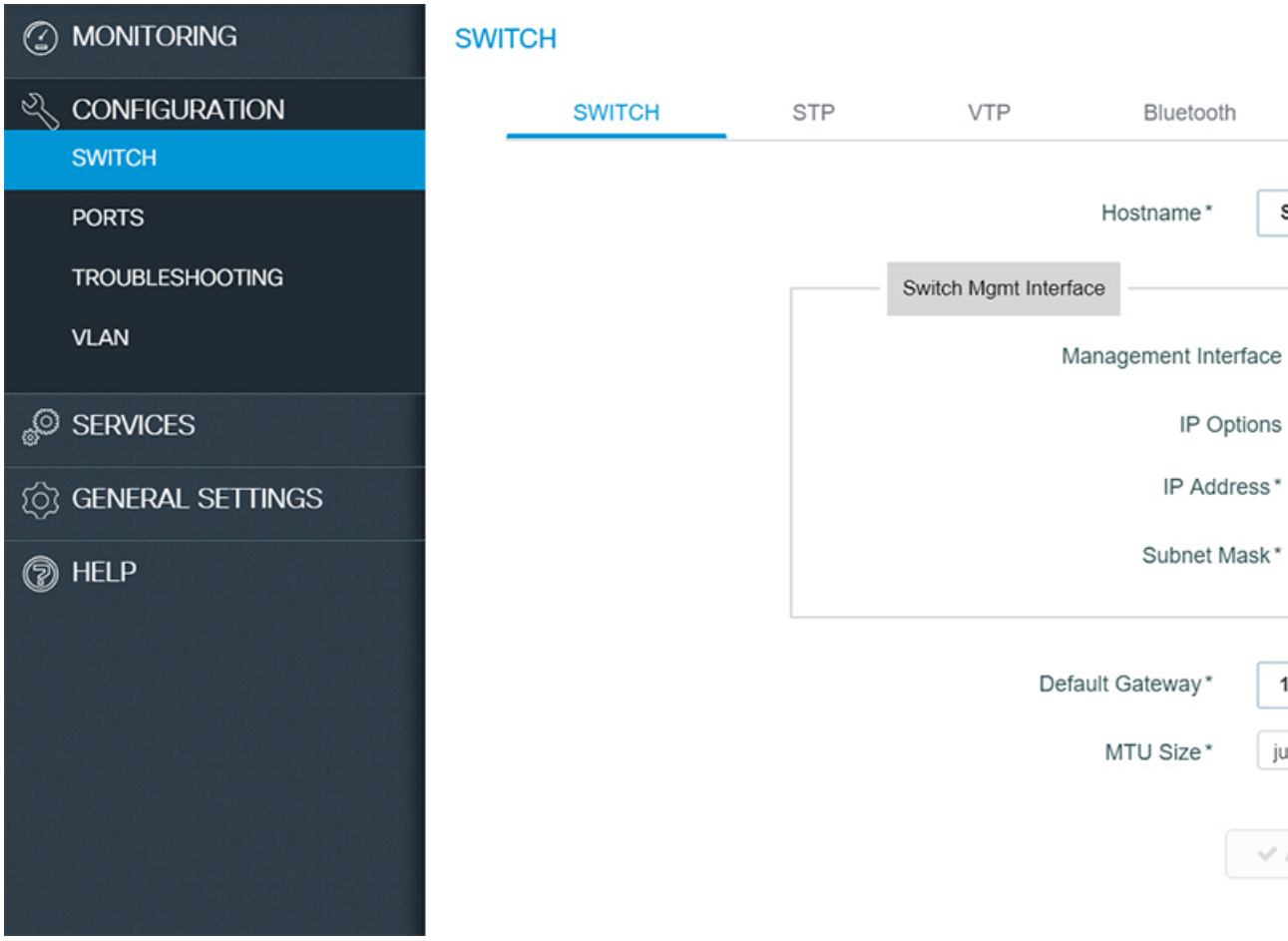
Configuring the Switch

Use the following sections to configure the switch.

Configuring Switch Details

The **Configuration > Switch > Switch** page allows you to configure access to the switch.

Figure 3: Configuring the Switch



Step 1 In the **Hostname** field, enter a hostname to identify your device on the network. It is case sensitive, can be alphanumeric, include special characters, and extend upto 32 characters.

Step 2 In the **Switch Management Interface** section, perform the following tasks to manage the switch remotely.

a) Enter a unique interface in the **Management Interface** field.

This management interface is used to access the user interface and remotely manage the switch. By default, it is VLAN1 because all ports are assigned to VLAN1. It is recommended to not use VLAN1 or VLANs that are used by client devices such as users and printers.

b) Select the **IP Options** checkbox to configure the IP addresses for the interface. You can configure both IPv4 and IPv6 addresses.

c) Assign an IP address in the **Switch IP Address** field.

d) Enter subnet mask details in the **Subnet** field.

e) For IPv6 address, select the type of IP address from the **Static** field.

- **Prefix**- Manually configures an IPv6 address on the interface. For example, 2001:0DB8:8086:6502::/32.

- **Anycast**- An anycast address is assigned to a set of interfaces that belong to different nodes. This ensures that when a packet is sent to an anycast address, the packet will be delivered to the closest interface configured with the anycst address.
- **eui-64**- Specifies a global IPv6 address with an extended unique identifier (EUI) in the low-order 64 bits of the IPv6 address. Specify only the network prefix; the last 64 bits are automatically computed from the switch MAC address. For example, 2001:0DB8:c18:1::/64 eui 64.
- **Link Local Address** - A unicast address that is automatically configured on an interface using the link-local prefix FE80::/10 and the interface identifier in the modified EUI-64 format. Using this address configuration option is sufficient for nodes on a link to communicate. For example, 2001:0DB8:c18:1:: link-local.

f) To use DHCP to assign an IPv6 address, choose **DHCP**. You can enable IPv6 DHCP Rapid Commit on the interface. To automatically configure the IPv6 address using stateless autoconfiguration on the interface and enable IPv6 processing on the interface, choose **Auto Config**.

Option	Description
Sample IPv4 Address	192.0.2.1
Sample IPv6 Address	2001:db8:0:1234:0:567:8:1
Sample Subnet Gateway	255.255.255.0
Sample MAC Address	AA:C3:EB:2E:1A:EF

Step 3 Enter the address of the interface through which the switch connects to the network in the **Default Gateway** field.

Step 4 Set the Maximum Transmission Unit (MTU) size in the **MTU Size** field. It is the largest sized packet that your device can send. If the connected router cannot handle a large MTU, packets may be retransmitted. A small MTU may result in a higher number of packets and cause overheads and performance limitations. The default value is 1500 bytes.

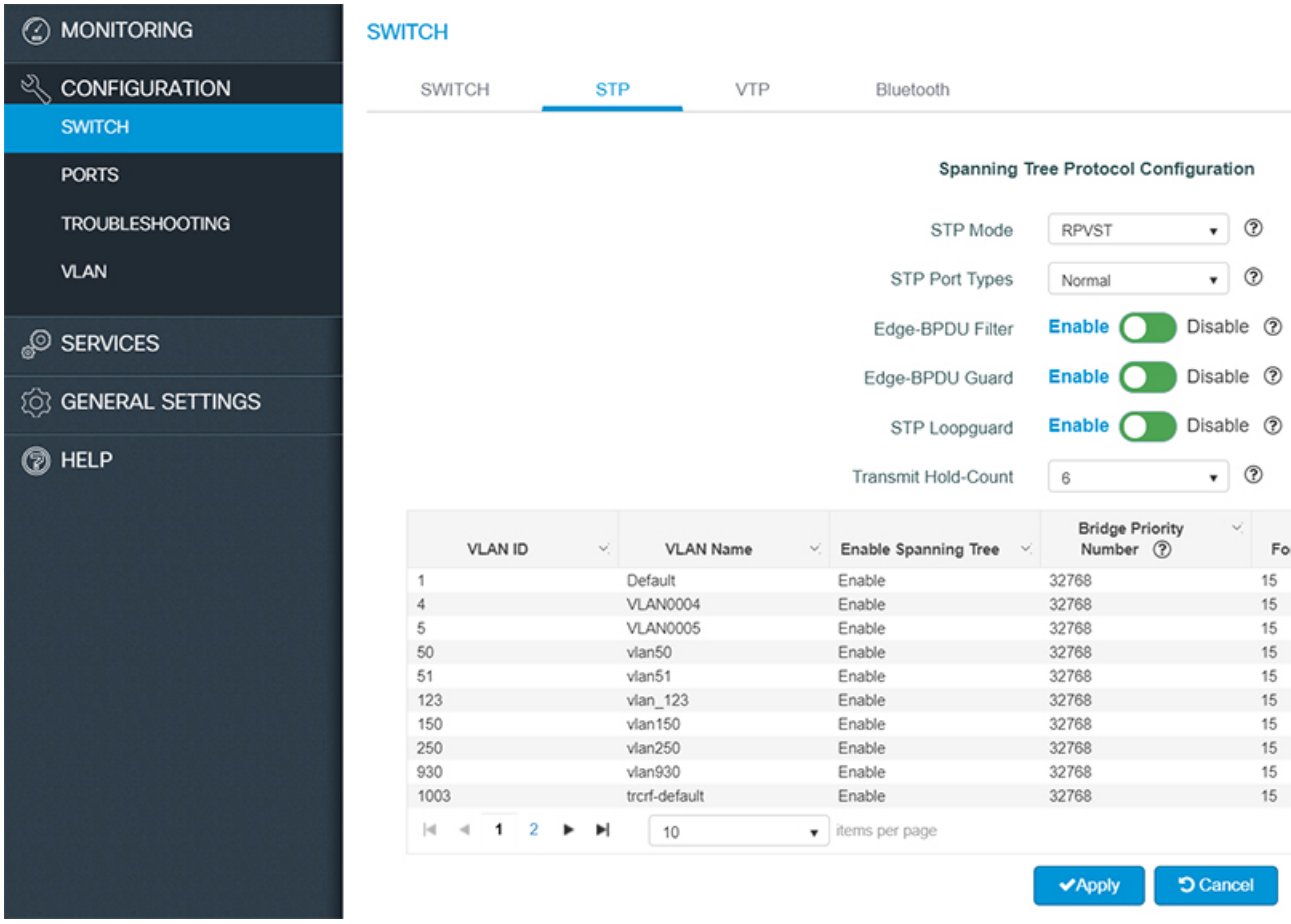
Step 5 Click **Apply** to save your changes.

Configuring STP

Spanning Tree Protocol (STP) is a network protocol that builds a logical loop-free topology for Ethernet networks.

The **Configuration > Switch > STP** page displays all the logical interfaces configured on your device. The default STP mode is RPVST.

Figure 4: STP



Step 1 From the **STP Mode** drop-down list, choose the STP mode for your device. Your device supports MST, PVST, and RPVST STP modes.

Step 2 In the **STP Port Types** drop-down list, select among Normal, Edge, or Network to enable portfast edge. MorePortFast causes the switch to enter the spanning tree forwarding state immediately, bypassing the listening and learning states.

Step 3 Select the interface for which you want to set the STP mode.

Step 4 Set the **Edge-BPDU Filter** toggle button to Enable to prevent the system from sending or even receiving BPDUs on specified ports. MoreSwitches send and receive spanning-tree frames, called bridge protocol data units (BPDUs), at regular intervals to ensure a loop-free path.

Step 5 Set the **Edge-BPDU Guard** toggle button to Enable to move a non-trunking port into an err-disable state when a BPDU is received on that port. MoreWhen you enable BPDU guard on the switch, spanning tree shuts down PortFast-configured interfaces that receive BPDUs instead of putting them into the spanning tree blocking state.

Step 6 Set the **STP Loopguard** toggle button to Enable to enable loopguard on the ports. MoreLoop guard helps prevent bridging loops that could occur because of a unidirectional link failure on a point-to-point link. It detects root ports and blocked ports and ensures that they keep receiving BPDUs from their designated port on the segment.

Step 7 Use the **Transmit Hold-Count** drop-down list to change the number of BPDUs that can be sent.

Step 8 To modify the bridge priority number, click the VLAN record in the list. Choose a new bridge priority number from the drop-down list.

To learn the topology of the network, STP-enabled switches communicate with each other using standardized data messages called BPDUs. Using BPDUs, the switch with the smallest bridge priority number is automatically elected as the root bridge. If the bridge priority is the same on all the switches then the switch with the smaller MAC address is elected as the root bridge. Each switch then elects port that are designated and that can communicate with th root bridge and forward traffic. Non-designated ports block traffic. A port normally starts in Blocking state, and then immediately moves through to the Listening state. In the Listening state, the device determines if the port is part of a physical loop. If it is, the port state is changed back to Blocking, and no data is sent or received on the port. If the port is not part of a loop, the port proceeds to the Learning state, and learns the MAC addresses in the frame. The port then moves into Forwarding state ready to send and receive data.

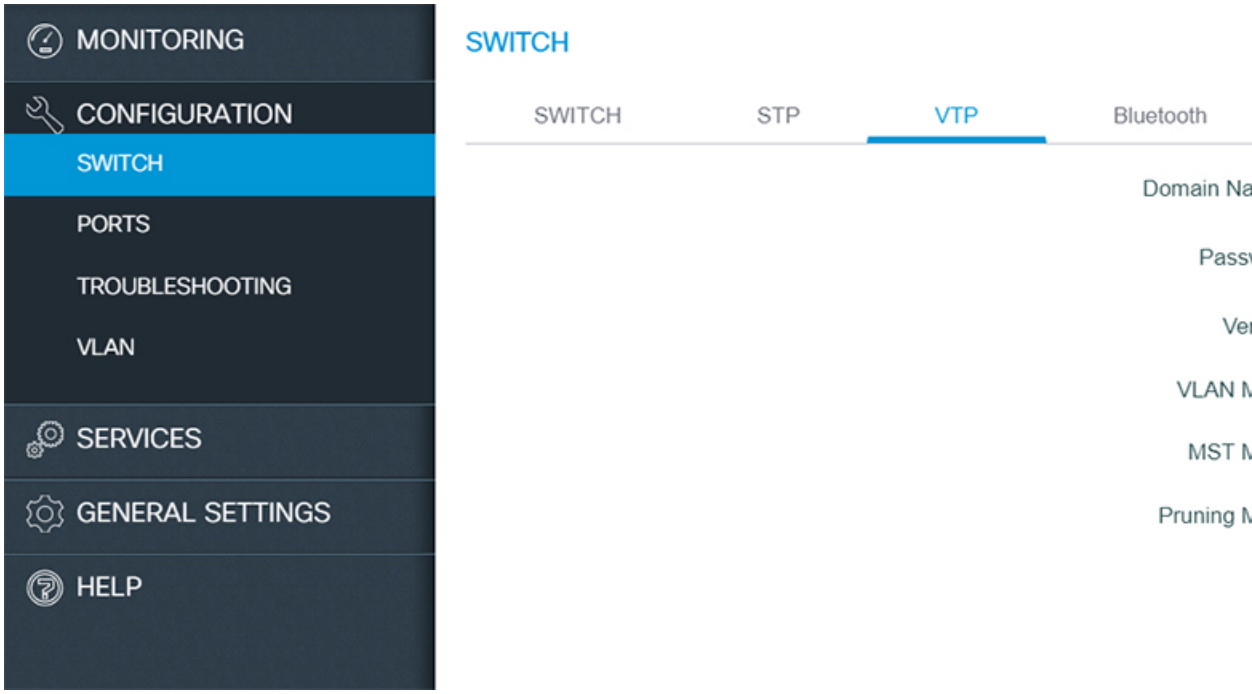
Step 9 Click **Apply**.

Configuring VTP

VTP reduces administration in a switched network. When you configure a new VLAN on one VTP server, the VLAN is distributed through all switches in the domain. This reduces the need to configure the same VLAN everywhere.

From the **Configuration > Switch > VTP** page:

Figure 5: Configuring VTP



Step 1 Enter a VTP administrative **Domain** name. The name can be 1 to 32 characters. All switches operating in VTP server or client mode under the same administrative responsibility must be configured with the same domain name.

Step 2 Enter the password for the VTP domain. The password can be 8 to 64 characters. If you configure a VTP password, the VTP domain does not function properly if you do not assign the same password to each switch in the domain.

Step 3 Select the version from the Version drop-down list. Version 3, provides enhanced authentication, support for extended range VLAN (VLANs 1006 to 4094) database propagation and support for any database in a domain for e.g. propagating Multiple Spanning Tree (MST) protocol database information.

Step 4 From the VLAN Mode select:

- Server - allows to change the VLAN configuration and have it propagated throughout the network. If you select server, this switch can be configured as the primary server.
- Client - does not allow to change its VLAN configuration. The client switch receives VTP updates from a VTP server in the VTP domain and then modifies its configuration accordingly.
- Transparent - switch continues to receive vlan database from other switches and forward those, but will not update VLAN database.
- Off - Same as VTP transparent mode except that VTP advertisements are not forwarded.

Step 5 From the **MST Mode**, select from the drop-down list. If you select server, this switch can be configured as the primary server for MST protocol database.

Step 6 Select the **Pruning Mode** checkbox to configure the domain to allow pruning.

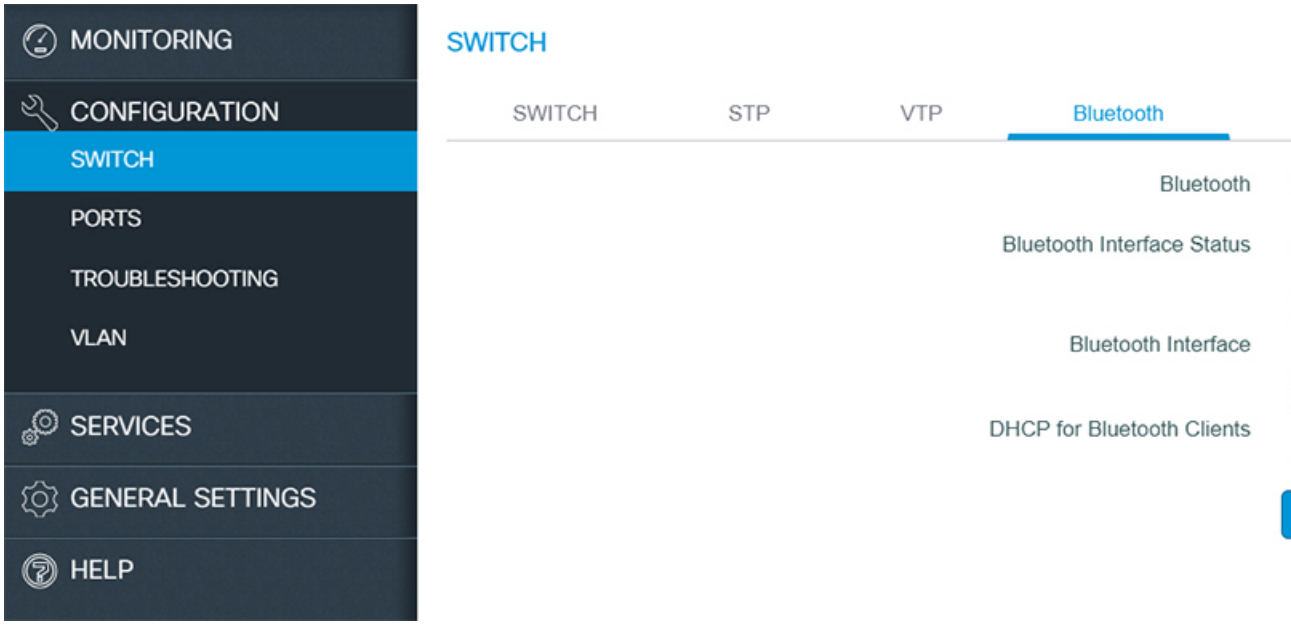
Step 7 Click **Apply** to save the changes.

Enabling Bluetooth

The switch can be configured and managed over the air with Bluetooth. The switch supports an external Bluetooth dongle that plugs into the USB port on the switch and allows Bluetooth based RF connection with external Laptops and Tablets.

The **Configuration > Switch > Bluetooth** tab is displayed only if your device supports Bluetooth. When your device boots up for the first time or after a factory reset, Bluetooth is enabled by default. However, immediately after the initial setup configuration is loaded, Bluetooth is disabled.

Figure 6: Enabling Bluetooth



To enable Bluetooth on your device, perform the following tasks on the **Configuration > Switch > Bluetooth** page:

Step 1 Set the **Bluetooth** field to *On*. The **Bluetooth Interface Status** indicates whether transfer through Bluetooth is possible or not.

Step 2 Enter the **IP Address** and the **Subnet Mask** for the Bluetooth interface.

Step 3 Enter the **DHCP Server** network address and the **Subnet Mask** for the Bluetooth interface. A new DHCP pool is created which is used to assign IP addresses to clients connecting through the Bluetooth interface. The Bluetooth interface IP address should ideally be the first IP address from this pool.

Configuring Ports

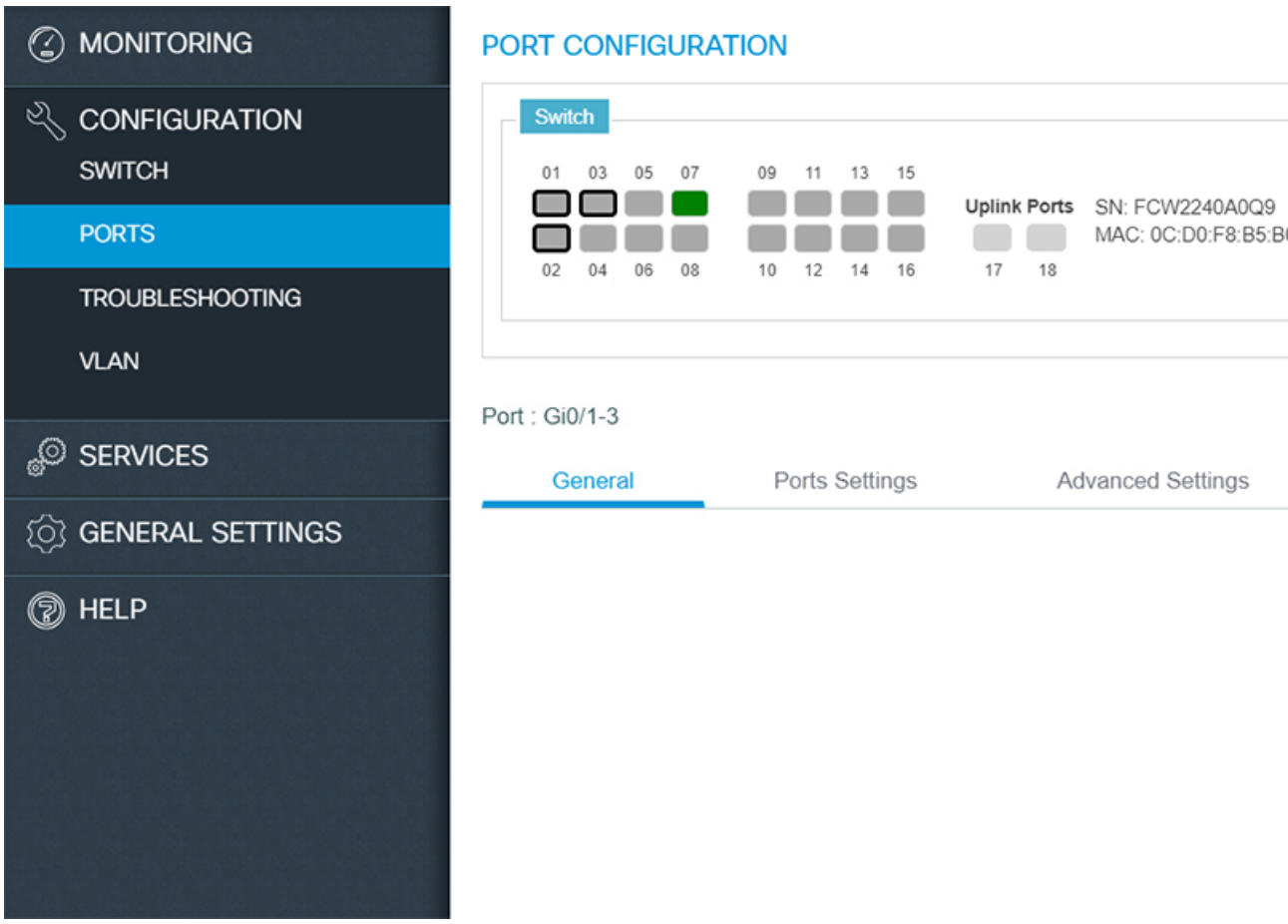
You can configure a port on the **Configuration > Ports > Port Configuration** page. By default, the first port is selected when you navigate to this page. You can select any other port by clicking on the switch view on the page. Additionally, you can view the port details by hovering over a port.

To configure settings for a port on your device, choose the port you want to configure from the ports displayed. The chosen port is outlined blue.

Configuring Port General Settings

Use this page to configure general port settings.

Figure 7: Configuring Port General Settings



Step 1 On the **Configuration** > **Ports** > **Port Configuration** page, choose the port you want to configure, and click the **General** tab.

Step 2 Choose *10 MB*, *100 MB*, or *1000 MB* as the interface speed, from the **Speed** drop-down list. To auto-negotiate the interface speed, and allow communicating ports to decide the optimum speed for transmission, choose *auto*.

Step 3 Choose *full*, *half*, or *auto* from the **Duplex** drop-down list.

- *Auto* auto-negotiates the interface mode, and allows communicating ports to decide the optimum mode for data transmission.
- Half-duplex communication is unidirectional, and the device cannot send and receive data simultaneously. This option can impact the performance of your device.
- Full-duplex communication increases effective bandwidth by allowing both ends of a connection to transmit and receive data simultaneously.

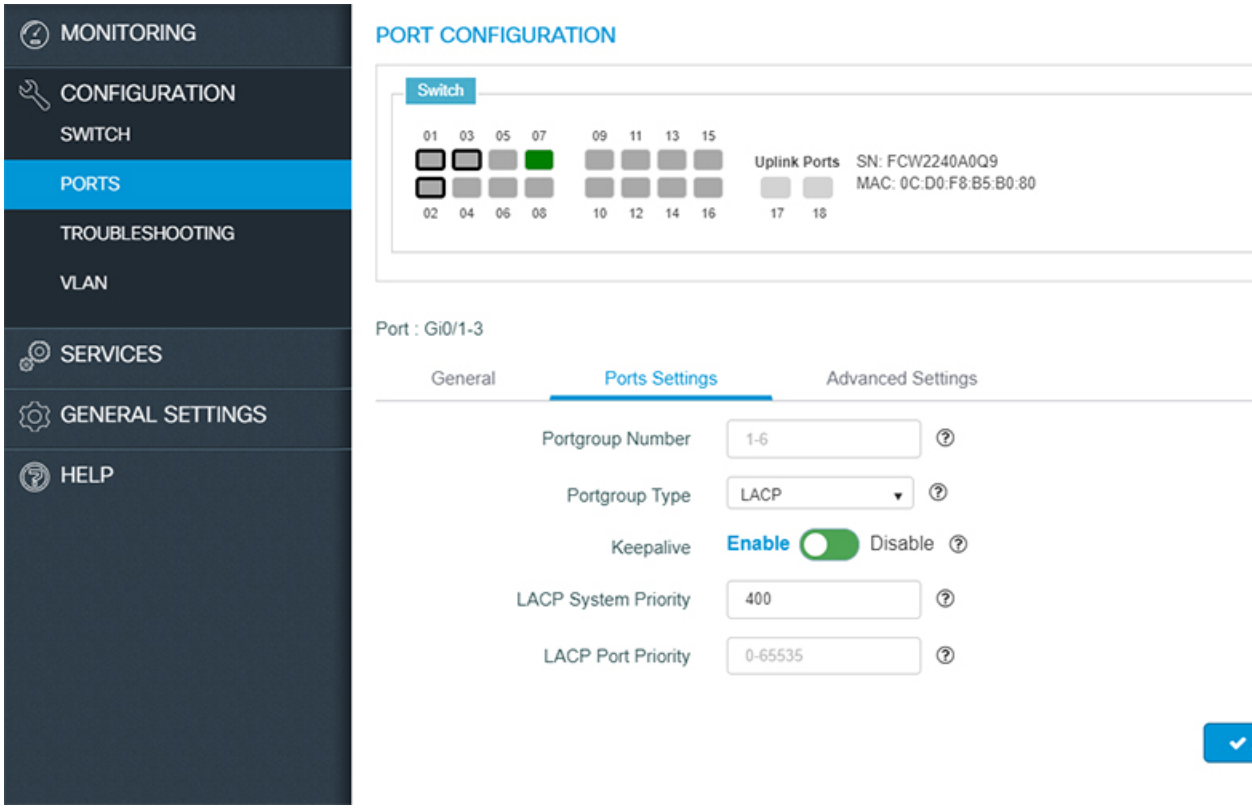
Step 4 To enable the interface on the device, set the **Status** field to *up*.

Step 5 Click **Apply** to save your changes.

Configuring EtherChannels

An EtherChannel or a port group is an aggregation of multiple physical interfaces that acts like a logical interface.

Figure 8: Configuring Port Settings - EtherChannels



Step 1 On the **Configuration** > **Ports** > **Port Configuration** page, choose the port you want to configure, and click the **Port Settings** tab.

Step 2 To add ports to a port group, hold the Ctrl key (on Microsoft Windows) or the Command key, and select multiple ports displayed in the switch view. Verify that the ports you selected are displayed.

Step 3 In the **Portgroup Number** field, enter the EtherChannel to which you want to add the selected ports.

When you add a port, it is first added to the default interface, after which the new configuration is applied. If you do not specify a port group number, the selected ports are configured with the same specified port settings, and no EtherChannel is created.

Step 4 From the **Portgroup Type** drop-down list, choose *PAgP* (Port Aggregation Protocol), *LACP* (Link Aggregation Control Protocol), or *On*. Ensure that you configure both ends of the EtherChannel with the same type.

When you configure one end of an EtherChannel in either PAgP or LACP mode, the device negotiates with the other end of the channel to determine which ports should become active. If the remote port cannot negotiate an EtherChannel, the local port is continues to carry data traffic as an independent port outside the EtherChannel.

When you configure an EtherChannel in the On mode, no negotiations take place. The device forces all compatible ports to become active in the EtherChannel.

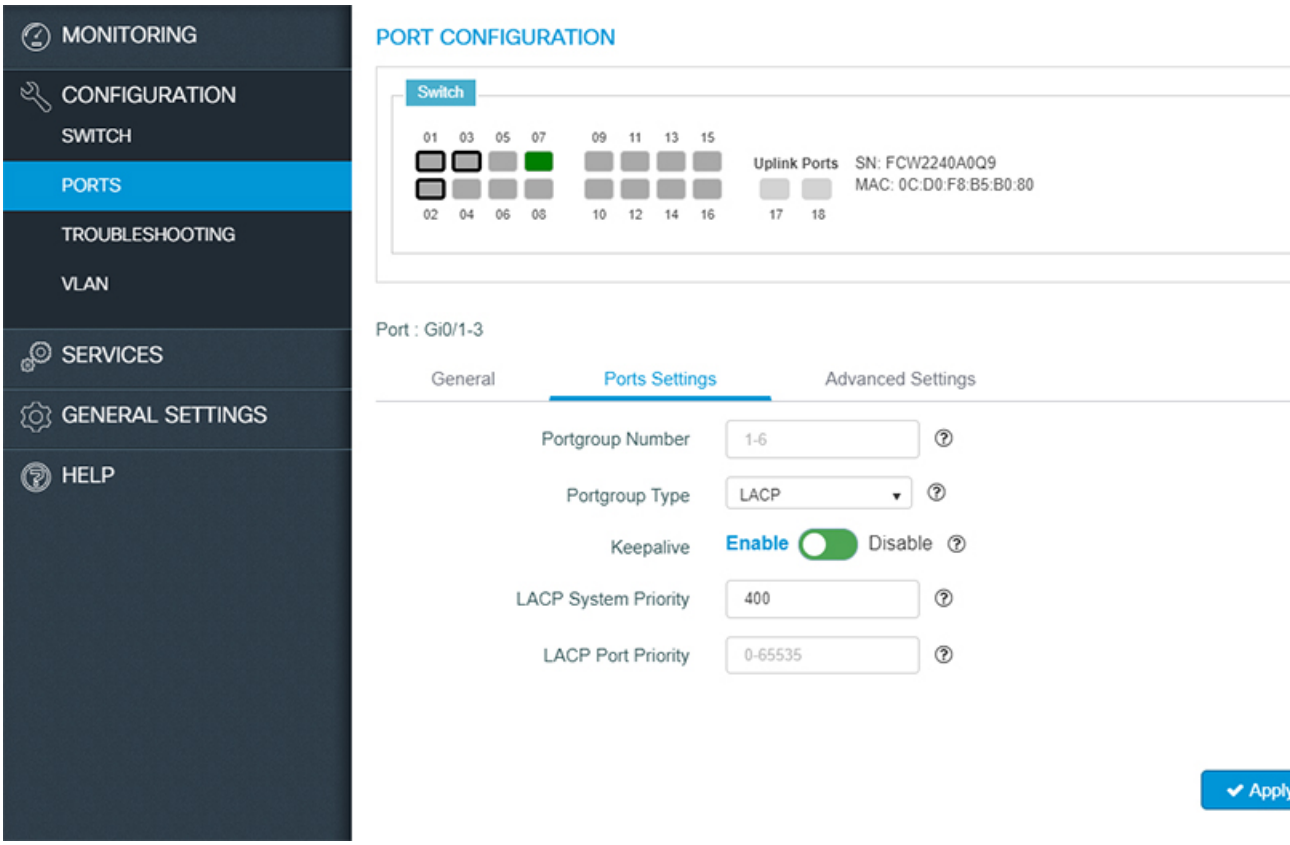
Step 5 Use the **Keepalive** field to configure the port mode. If you choose PAGP as the port group type, and set the **Keepalive** field to *On*, the port is configured in *desirable mode*. If **Keepalive** is *Off* the port mode is set to *auto*. If you chose LACP as the port group type, and set **Keepalive** field to *On*, the port is configured in *active mode*. If **Keepalive** field is *Off* the port mode is set to *auto*.

Step 6 Enter an LACP priority value at the device level using the **LACP System Priority** field or at the port level using the **LACP Port Priority** field.

Step 7 Click **Apply** to save your changes.

Configuring Port Settings - Layer 2 Interface

Figure 9: Configuring Port Settings - Layer2



Step 1 On the **Configuration** > **Ports** > **Port Configuration** page, choose the port you want to configure, and click the **Port Settings** tab.

Step 2 Choose a switch mode.

Access ports transport traffic to and from only the VLAN assigned to it.

Trunk ports carry traffic for multiple VLANs, using a process called trunking. Trunk ports mark frames with unique identifying IEEE 802.1Q tags (when configured), to direct each frame to its designated VLAN.

When a port is in *dynamic auto* mode, it passively listens for and receives Dynamic Trunking Protocol (DTP) messages generated by a port in *dynamic desirable* mode, on another switch on the other side. A trunk link is formed between the two interfaces and all frames are tagged.

Step 3 If you choose *access* mode, assign a VLAN to the port, in the **Access VLAN** field. By default, all ports assigned to VLAN 1 are assigned as access ports.

Step 4 If you choose *trunk* as the switch mode, assign a range of VLANs to the port. To assign all VLANs to carry port traffic, select **All VLANs**, or select **VLAN IDs** and specify a range of VLANs that can carry traffic for the port.

Step 5 If you choose *dynamic auto* or *dynamic desirable*, assign a range of VLANs to the port. To assign all VLANs to carry port traffic, select **All VLANs**, or select **VLAN IDs** and specify a range of VLANs that can carry traffic for the port. If DTP negotiation fails, the dynamic auto and dynamic desirable ports become access ports. Assign an access VLAN to the ports, in the **Access VLAN** field.

Step 6 In the **Voice VLAN** field, specify a VLAN to carry voice traffic.

Step 7 For network security reasons, specify a VLAN other than VLAN 1 in the **Native VLAN** field. When your device receives untagged frames on a trunk port, they are sent to the native VLAN. By default, this is VLAN 1.

Step 8 If your device connects to endpoints (for example, to phones and computers and not to other switches or hubs), set the **Port Fast** field to *on*, to enable PortFast on the interface.

Devices that connect to PortFast enabled ports can connect to the network immediately, instead of waiting for the port to transition from the listening and learning states to the forwarding state.

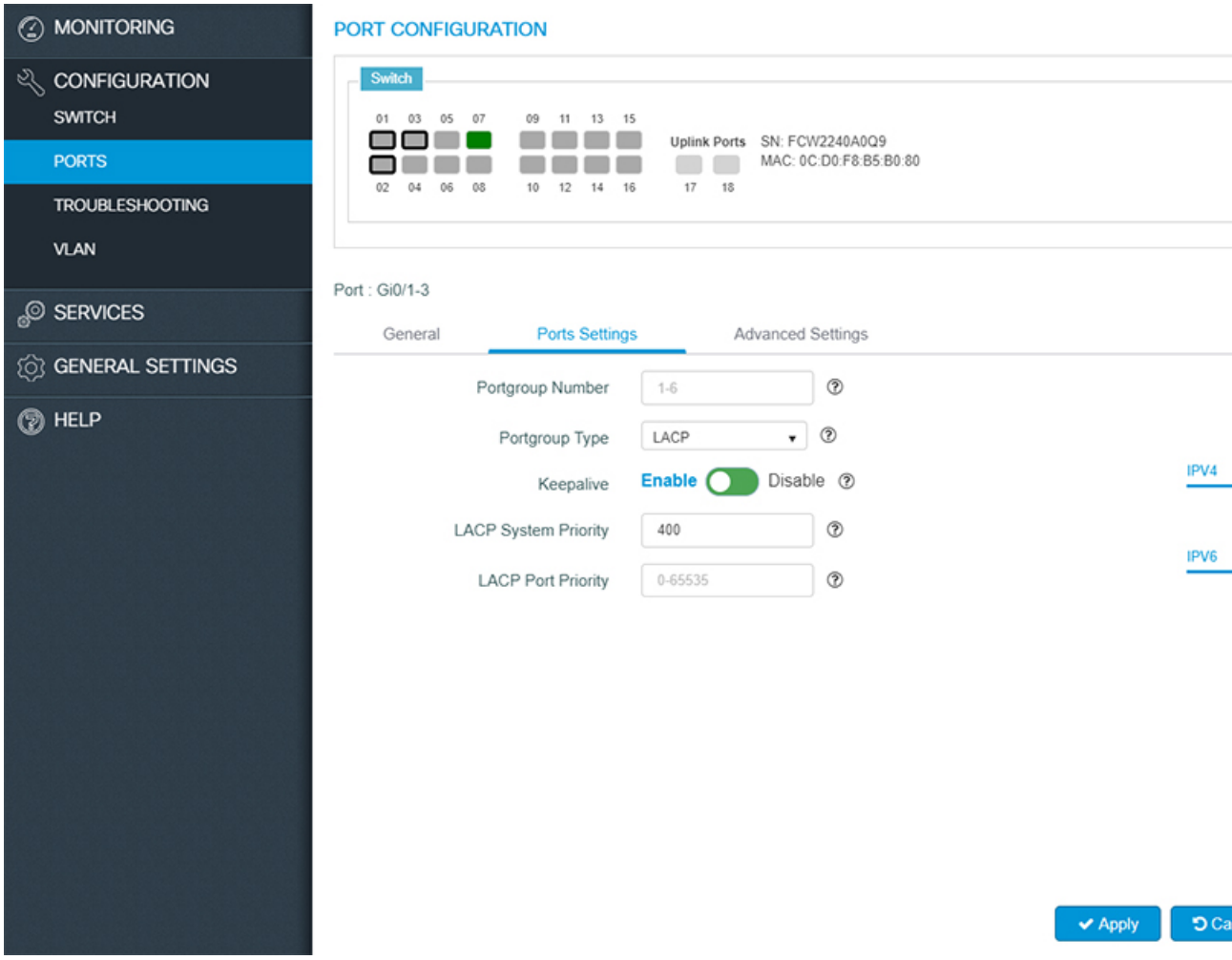
Step 9 To activate DHCP snooping on the port, set **DHCP Snooping** to *enable*. DHCP snooping acts like a firewall between untrusted hosts and trusted DHCP servers, validating DHCP messages received from untrusted sources and filtering out invalid messages. The DHCP snooping binding database maintains information about untrusted hosts with leased IP addresses, and validates subsequent requests from untrusted hosts.

Step 10 Click **Apply** to save your changes.

Configuring Port Settings - Layer 3 Interface

A routed interface is a physical port that can route IP traffic to another device. To configure a Layer 3 interface:

Figure 10: Configuring Port Settings - Layer3



Step 1 On the **Configuration** > **Ports** > **Port Configuration** page, choose the port you want to configure, and click the **Port Settings** tab.

Step 2 Slide to select **Routed** mode.

Step 3 Assign an IP address to this interface. You can assign both IPv4 and IPv6 addresses.

a) To specify an IPv4 address and subnet mask for the interface, choose **Static IP**, from the **IP Type** drop-down list.

b) To use DHCP to assign an IP address to the interface, choose **DHCP** from the **IP Type** drop-down list. Specify a hostname.

c) To use an IP address from a DHCP pool, choose **DHCP Pool** from the drop-down list.

d) For IPv6 address, select the type of IP address from the **Static** field.

- **Prefix**- Manually configures an IPv6 address on the interface. For example, 2001:0DB8:8086:6502::/32.
- **Anycast**- An anycast address is assigned to a set of interfaces that belong to different nodes. This ensures that when a packet is sent to an anycast address, the packet will be delivered to the closest interface configured with the anycst address.

- **eui-64**- Specifies a global IPv6 address with an extended unique identifier (EUI) in the low-order 64 bits of the IPv6 address. Specify only the network prefix; the last 64 bits are automatically computed from the switch MAC address. For example, 2001:0DB8:c18:1::/64 eui 64.
- **Link Local Address** - A unicast address that is automatically configured on an interface using the link-local prefix FE80::/10 and the interface identifier in the modified EUI-64 format. Using this address configuration option is sufficient for nodes on a link to communicate. For example, 2001:0DB8:c18:1:: link-local.

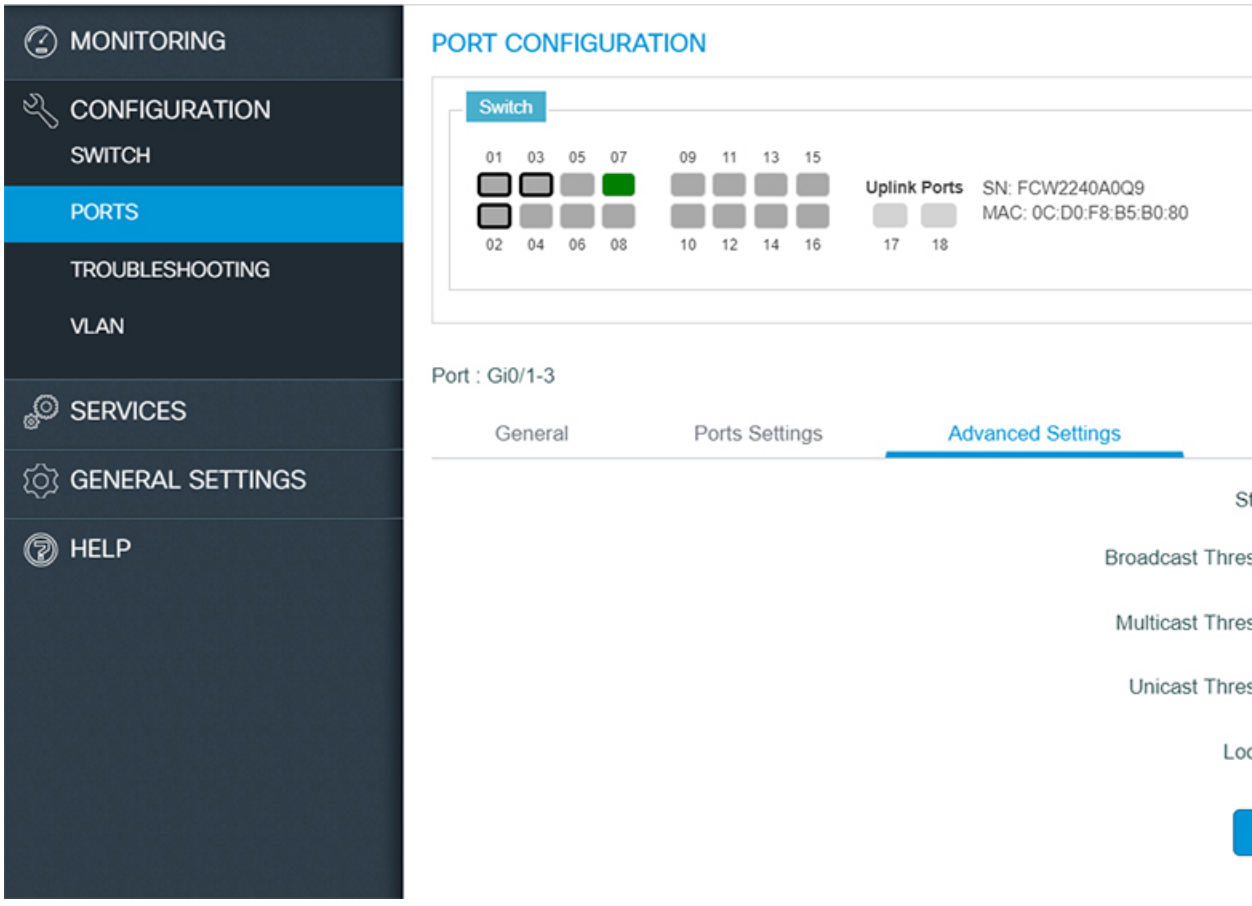
e) To use DHCP to assign an IPv6 address, choose **DHCP**. You can enable IPv6 DHCP Rapid Commit on the interface. To automatically configure the IPv6 address using stateless autoconfiguration on the interface and enable IPv6 processing on the interface, choose **Auto Config**.

Step 4 Click **Apply** to save your changes.

You can configure the same IP address on multiple ports, which are in **Admin Down** state, using the Web UI. No warning message is shown for ports in **Admin Down** state. You can bring **UP** only one port. If you try to bring up the other port, an error message is shown.

Configuring Port Advanced Settings

Figure 11: Configuring Port Advanced Settings



Step 1 On the **Configuration** > **Ports** > **Port Configuration** page, choose the port you want to configure, and click the **Advanced Settings** tab.

Step 2 Storm control prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on a port. From the **Storm Control** drop-down list:

- To error-disable the port during a storm, choose *Shutdown*.
- To generate an SNMP trap when a storm is detected, choose *Trap*.
- To disable storm control, choose *None*.

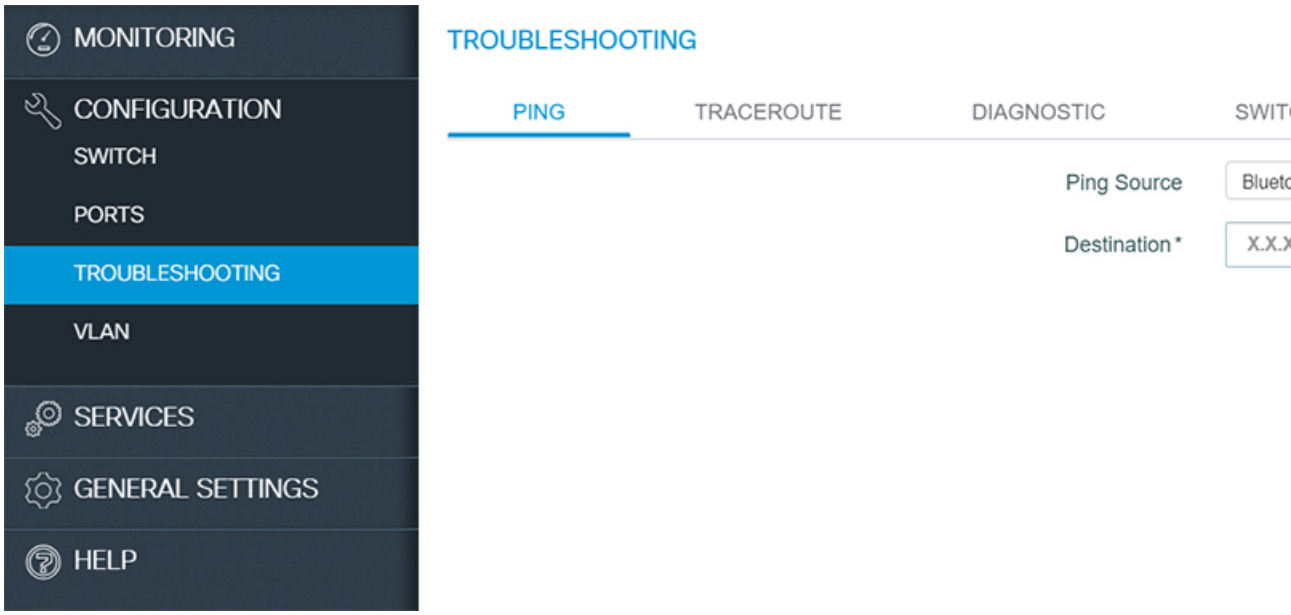
Step 3 Specify thresholds for unicast, broadcast, and multicast traffic entering your device. These values indicates the number of packets allowed per second, as part of your unicast, broadcast, and multicast traffic.

Step 4 Click **Apply** to save your changes.

Troubleshooting the Device

To troubleshoot network reachability, communication delays, and packet loss, use the **Configuration > Troubleshooting** page.

Figure 12: Troubleshooting



Troubleshooting Using Ping

On the **Troubleshooting > Ping** page, choose the interface from which to send ping packets to the specified destination, and click **Ping**.

Troubleshooting Using Traceroute

On the **Troubleshooting > Traceroute** page, enter the destination address for which you want to run traceroute, and click **Traceroute**. Traceroute discovers the route, and the number of hops that packets take when traveling to their destination and helps you identify potential link bottlenecks throughout the transmission path.

Running Diagnostics

On the **Troubleshooting > Diagnostics** page, choose the type of tests to run on the switch, and click **Start**. Running some diagnostic tests may be disruptive to the switch.

Rebooting the Device

Use the **Troubleshooting > Switch Reboot** page, to restart the switch or restore it to factory defaults.

- **Restart Switch** - Click to reboot the switch. You can select to restart the switch on the **Restart Switch** dialog box with or without saving the recent configurations. If you do not select the **Save Configuration** check box, the switch is restarted with the existing configurations.
- **Factory Reset** - Click to erase the startup configuration in the persistent memory on the switch and reboot it with the initial factory default configuration. After you reset a switch, you can not recover the erased configuration.

Working with Logs

On the **Troubleshooting > Logs** page, use the **Config Logs** button to configure the type and details of logs that you want to see and click the **Save & Apply to Device** button. Also, you can set a numerical value to the number of latest log entries to display. You can download the logs for further troubleshooting.

Working with Debug

You can view and download debug reports on the **Troubleshooting > Debug** page. Assign a name using the **Name of the debug output** field. In the **Enter the CLIs of which output needs to be packaged** field, enter up to five CLIs. To view the output in the same window, click **View**, else click **Download Output** to save the report as a text file.

Configuring VLAN

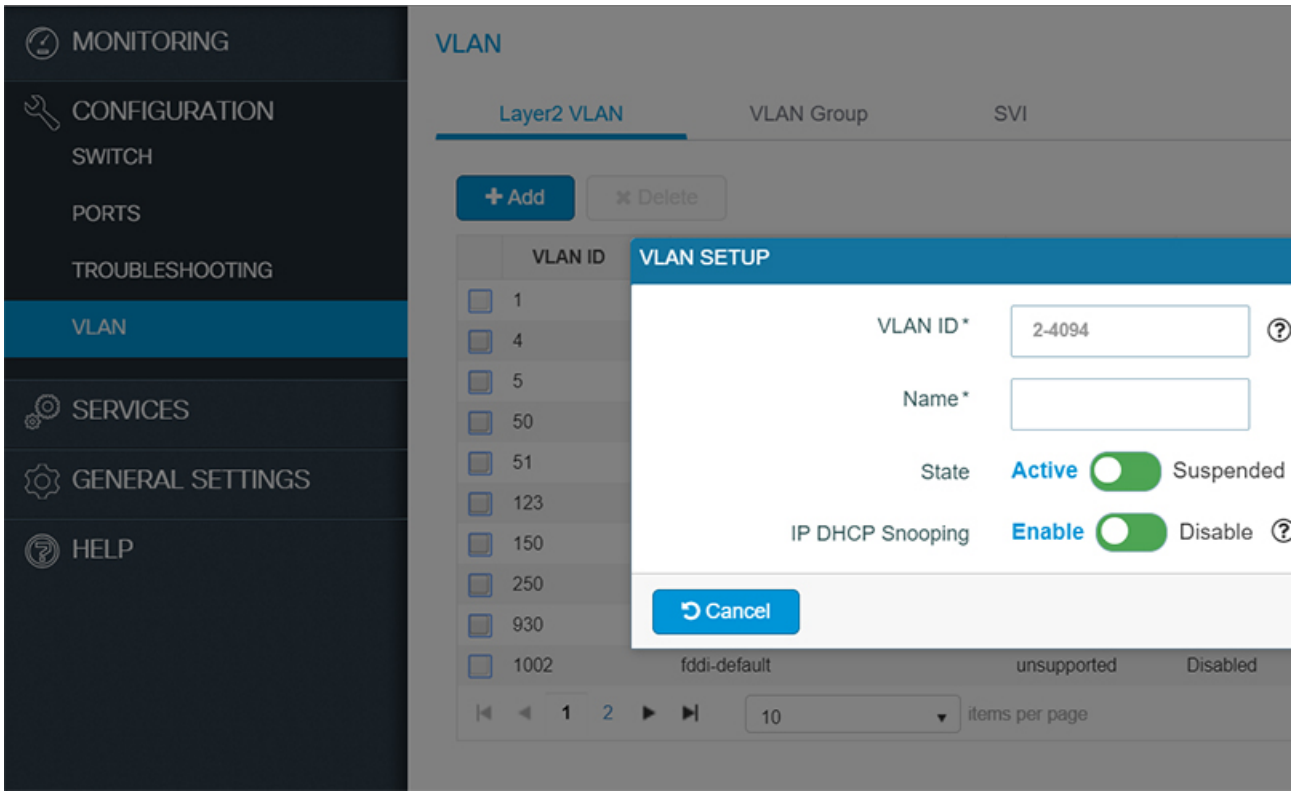
A VLAN or a virtual LAN is a group of devices on one or more LANs, which are configured to communicate as if they were physically connected, despite being located across LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

Using VLANs you can partition your network based on functional and security requirements within your organization, without investing in new cables and without making major changes to current network infrastructure. For example, VLANs can be created to divide your network into logical groups, and secure traffic to and from departments such as Finance or Marketing. VLANs could also be created to restrict the use of resources such as file servers and printers to a logical group of users on your network.

As defined by the IEEE 802.1Q standard, the VLAN identifier or tag consists of 12 bits in the Ethernet frame, creating an inherent limit of 4,096 VLANs on a LAN.

Configuring Layer 2 VLANs

Figure 13: Configuring Layer2 VLAN



Step 1 On the**Configure** > **VLAN** page, click the **Layer2 VLAN** tab. To add a Layer 2 VLAN, click **Add**. To edit a VLAN, select the VLAN ID in the table. Details of the VLAN are displayed in the **VLAN SETUP** section.

Step 2 In the **VLAN ID** field, enter an ID between 2 and 4094, to identify the VLAN on your network. VLAN 1 is the default VLAN on your device.

Step 3 Enter a name to identify the VLAN.

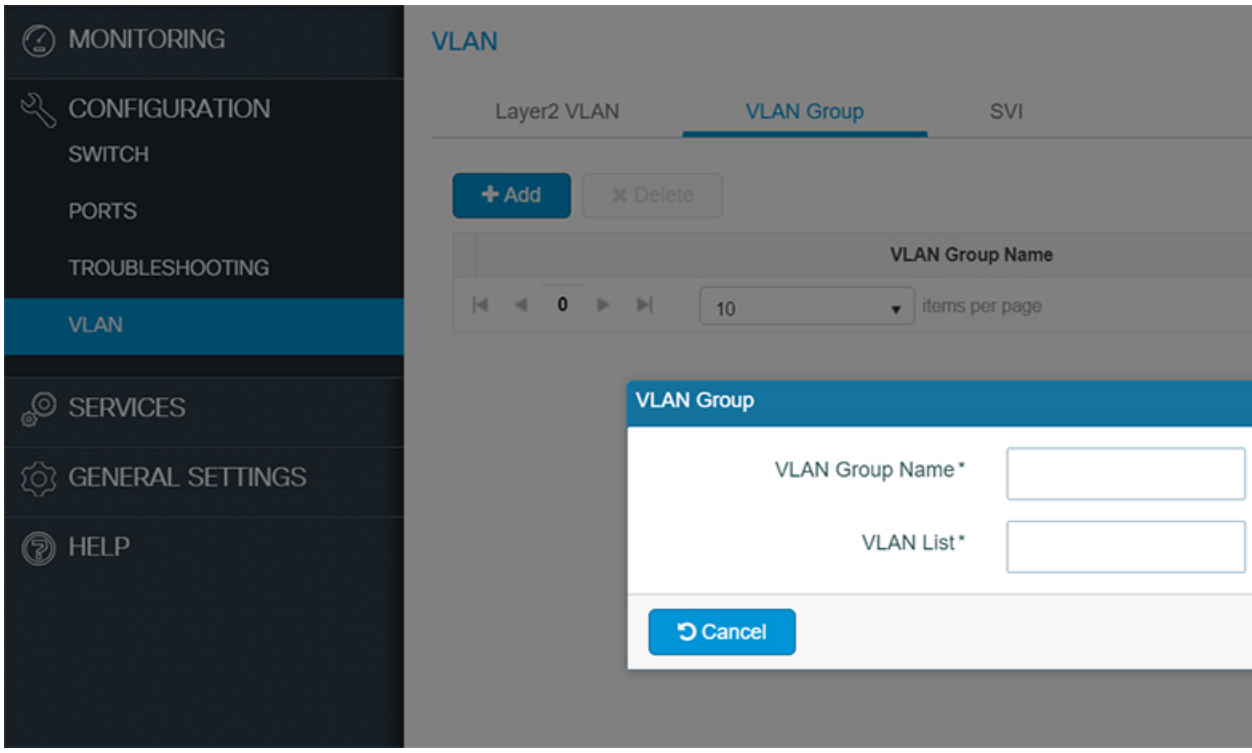
Step 4 Set the **State** toggle button to **Active** to forward traffic through the VLAN. VLANs in *suspended* state cannot forward traffic on your device.

Step 5 Set the **IP DHCP Snooping** toggle button to **Enable**, to validate DHCP messages received from untrusted sources and filter them out.

Step 6 Click **Apply** to save your changes.

Configuring VLAN Group

Figure 14: Configuring VLAN Group



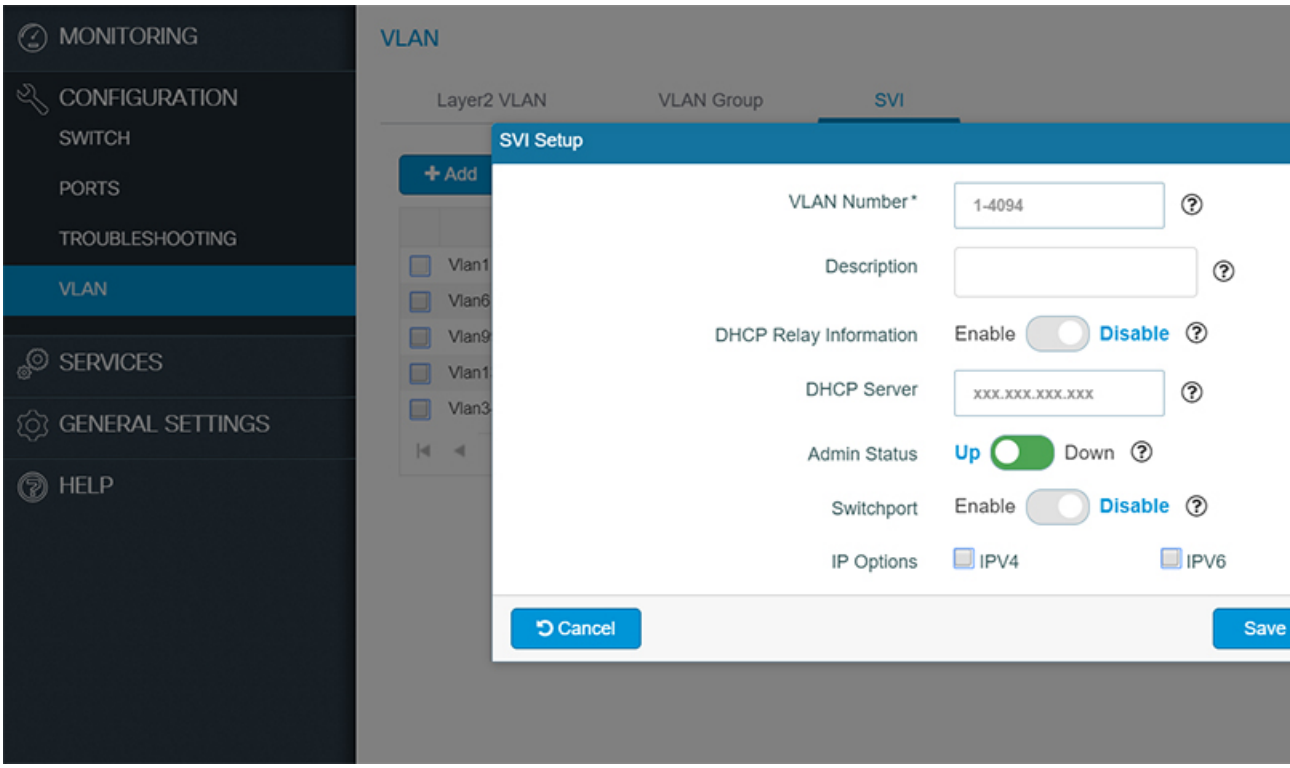
Step 1 On the **Configuration > VLAN > VLAN Group** page, click **Add** to create a VLAN Group. A VLAN group is a logical container for all the VLANs and ensures that the configured parameters are applicable to all the VLANs belonging to this group.

Step 2 Specify a group name and add a list of VLANs to this group. The number of VLANs must not exceed 32.

Step 3 Click **Save**.

Configuring Switch Virtual Interface

Figure 15: Configuring SVI



Step 1 On the **Configuration > VLAN > SVI** page, click **Add**. In the **SVI Setup** window, type an ID between 1 and 4095, to associate the ID with the VLAN on your network in the **VLAN Number** field.

Step 2 Enter the Description of the VLAN interface.

Step 3 Set **DHCP Relay Information** to **Enable**, to forward DHCP packets between the server and the client. However to do so, the IP address of the DHCP server must be configured on the SVI of the DHCP client.

Step 4 Enter the details of the DHCP Server.

Step 5 Set **Admin Status** to **Up**.

Step 6 Configure the IP address on the SVI. You can configure both IPv4 and IPv6 addresses.

a) For IPv4, enter the IP Address and Subnet Mask.

b) For IPv6 address, select the type of IP address from the **Static** field.

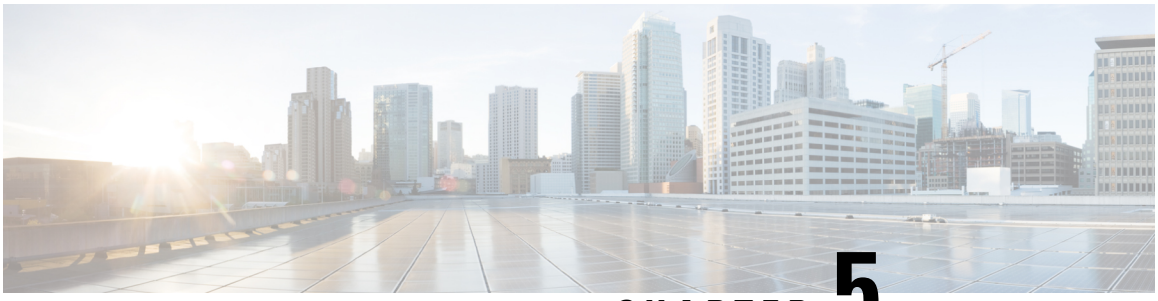
- **Prefix**- Manually configures an IPv6 address on the interface. For example, 2001:0DB8:8086:6502::/32.
- **Anycast**- An anycast address is assigned to a set of interfaces that belong to different nodes. This ensures that when a packet is sent to an anycast address, the packet will be delivered to the closest interface configured with the anycst address.
- **eui-64**- Specifies a global IPv6 address with an extended unique identifier (EUI) in the low-order 64 bits of the IPv6 address. Specify only the network prefix; the last 64 bits are automatically computed from the switch MAC address. For example, 2001:0DB8:c18:1::/64 eui 64.

- **Link Local Address** - A unicast address that is automatically configured on an interface using the link-local prefix FE80::/10 and the interface identifier in the modified EUI-64 format. Using this address configuration option is sufficient for nodes on a link to communicate. For example, 2001:0DB8:c18:1:: link-local.

Step 7 Click **Save & Apply to Device**.

PART V

Services



CHAPTER 5

Configuring Services

Configuring Static Routing

Use static routes in environments where network traffic is predictable and where the network design is simple. Routers forward packets using either route information from route table entries that you manually configure or the route information that is calculated using dynamic routing algorithms. Static routing is the simplest form of routing, where you manually enter routes into a routing table.

Static routes define explicit paths between two routers, and cannot be automatically updated. You must manually reconfigure static routes when network changes occur.

Figure 16: Configuring Static Routing - IPv4

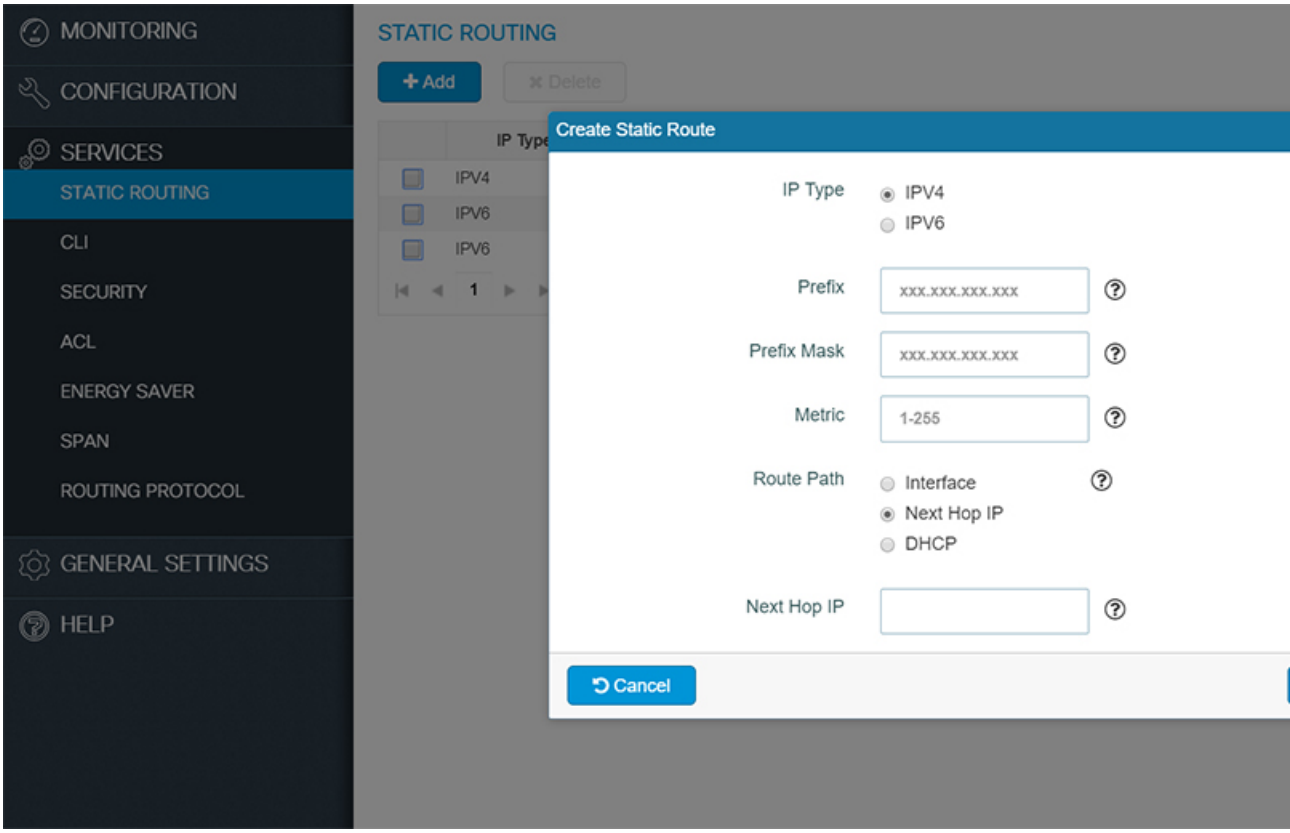
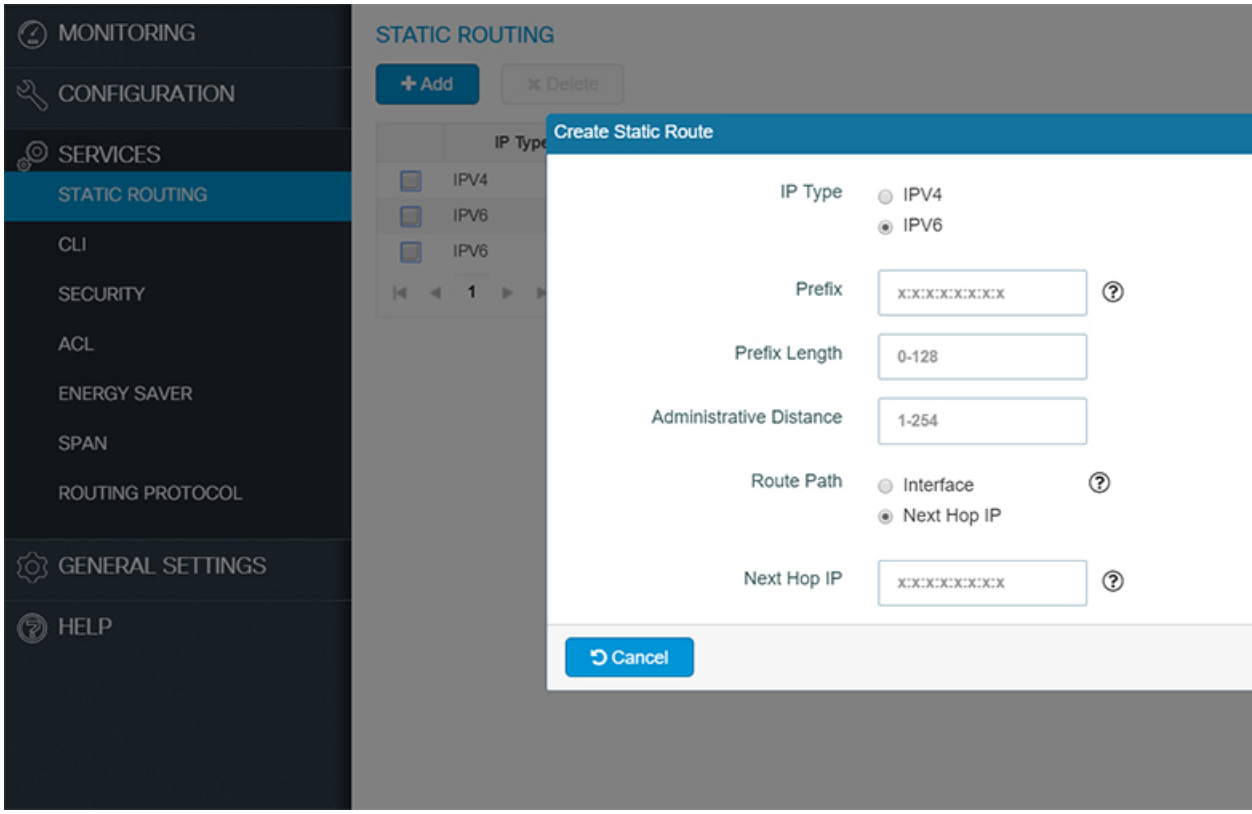


Figure 17: Configuring Static Routing - IPv6



Step 1 Choose **Services > Static Routing**, and click **Add**.

Step 2 In the **Create Static Route** window, select **IP Type** for **IPv4** or **IPv6** address.

Step 3 For provisioning static routing using IPv4 address:

a) In the **Prefix** and **Prefix Mask** fields, enter the IP address and the subnet mask for the static route.

b) In the **Metric** field, assign a metric, between 1 and 255, to the static route.

When multiple paths to the same destination are available, the device uses the route with the lowest metric and adds the preferred route into the routing table.

c) In the **Route Path** field, choose one of the following options:

- *Interface* — To indicate the output interface, that is the interface on which all packets are sent to the destination network. Choose an interface from the **Interface** drop-down list. In the **Next Hop IP** field, assign a next-hop IP address to the output interface.
- *Next Hop IP* — To specify a next-hop IP address for the static route. Assign a next-hop IP address in the **Next Hop IP** field.
- *DHCP* — To assign a static route IP address using a DHCP server.

The route is removed when the DHCP lease expires. Using DHCP to determine a route path eliminates the need to configure static routes to an outside interface and the configuration of a next-hop router.

Step 4 For provisioning static routing using IPv6 address:

a) In the **Prefix** field, enter the IPv6 address to manually configure it on the interface.
b) In the **Prefix Length** field, enter the value in bits, between 1 and 128.

Prefix length is the number of bits set in the subnet mask. For example, in the IP address 2001:0DB8:8086:6502::/32, 2001:0DB8:8086:6502 is the prefix, and 32 is the prefix length.

c) In the **Administrative Distance** field, enter a value to determine the routing protocol.

It is used to rank routes when multiple paths to the same destination are available. Routes with smaller administrative distances are preferred.

d) In the **Route Path** field, choose one of the following options:

- *Interface* — To indicate the output interface, that is the interface on which all packets are sent to the destination network. Choose an interface from the **Interface** drop-down list. In the **Next Hop IP** field, assign a next-hop IP address to the output interface.
- *Next Hop IP* — To specify a next-hop IP address for the static route. Assign a next-hop IP address in the **Next Hop IP** field.

Step 5 Click **Save** to save the static route.

About Security Configuration

AAA (Authentication, Authorization, and Accounting) is an architectural framework for configuring a set of three independent security functions in a consistent manner. AAA provides a modular way of performing the following services:

- **Authentication**—Provides the method of identifying users, including login and password dialog, challenge and response, messaging support, and, depending on the security protocol you select, encryption. Authentication is the way a user is identified prior to being allowed access to the network and network services. You configure AAA authentication by defining a named list of authentication methods, and then applying that list to various interfaces.
- **Authorization**—Provides the method for remote access control, including one-time authorization or authorization for each service, per-user account list and profile, user group support, and support of IP, IPX, ARA, and Telnet.

  AAA authorization works by assembling a set of attributes that describe what the user is authorized to perform. These attributes are compared to the information contained in a database for a given user and the result is returned to AAA to determine the user's actual capabilities and restrictions. The database can be located locally on the access server or router or it can be hosted remotely on a RADIUS or TACACS+ security server. Remote security servers, such as RADIUS and TACACS+, authorize users for specific rights by associating attribute-value (AV) pairs, which define those rights with the appropriate user. All authorization methods must be defined through AAA.

  As with authentication, you configure AAA authorization by defining a named list of authorization methods, and then applying that list to various interfaces.
- **Accounting**—Provides the method for collecting and sending security server information used for billing, auditing, and reporting, such as user identities, start and stop times, executed commands (such as PPP), number of packets, and number of bytes.

Accounting enables you to track the services users are accessing as well as the amount of network resources they are consuming. When AAA accounting is activated, the network access server reports user activity to the RADIUS or TACACS+ security server (depending on which security method you have implemented) in the form of accounting records. Each accounting record is comprised of accounting AV pairs and is stored on the access control server. This data can then be analyzed for network management, client billing, and/or auditing. All accounting methods must be defined through AAA. As with authentication and authorization, you configure AAA accounting by defining a named list of accounting methods, and then applying that list to various interfaces.

In many circumstances, AAA uses protocols such as RADIUS, TACACS+, or Kerberos to administer its security functions. If your device acts as a network access server, AAA is the means through which you establish communication between your network access server and your security server.

Configuring Security

To use the AAA feature, you can enable it on the **Services > Security > AAA Server** page. After enabling, you need to set up the authentication servers that contain the AAA database.

Configure RADIUS Servers

Step 1 On the **Services > Security > AAA Server** page, click **Add**.

Step 2 Select the authentication protocol from the **Protocol** drop-down list.

Step 3 Enter a name for the server and, and enter the IP address in the **Server Address** field.

Step 4 In the **Shared Secret** field, enter the shared secret key to be used for authentication between the server and your device. Confirm the shared secret.

Step 5 In the **Auth Port** and **Acct Port** fields, enter the RADIUS server's UDP port numbers. The valid range is 1 to 65535, and the default value is 1812 for authentication and 1813 for accounting.

Step 6 Click **Save & Apply to Device**.

Configure TACACS+ Server

Step 1 On the **Services > Security > AAA Server** page, click **Add**.

Step 2 Enter a name for the server and, and enter the IP address in the **Server Address** field.

Step 3 In the **Shared Secret** field, enter the shared secret key to be used for authentication between the server and your device. Confirm the shared secret.

Step 4 In the **Port** field, enter the TACACS server's UDP port number. The valid range is 1 to 65535, and the default value is 49.

Step 5 Click **Save & Apply to Device**.

Configure LDAP Server

Step 1 On the **Services > Security > AAA Server** page, click **Add**.

Step 2 Enter a name for the server and, and enter the IP address in the **Server Address** field.

Step 3 In the **Port** field, enter the LDAP server's UDP port number. The valid range is 1 to 65535, and the default value is 389.

Step 4 In the **User Base DN** field, enter the distinguished name (DN) of the subtree in the LDAP server that contains a list of all the users. For example, ou=organizational unit, .ou=next organizational unit, and o=corporation.com. If the tree containing users is the base DN, type. o=corporation.com, or dc=corporation, dc=com.

Step 5 Click **Save & Apply to Device**.

What to do next

The configured list of AAA servers along with their name, address and protocol are displayed in the table listed on the page. If you need to check the status of a server, click **Ping**.

Configure Access Policy

You can configure any combination of the following authentication and authorization methods to control administrative login access to a switch.

Step 1 On the **Services > Security > Access Policy** page, click **Add**.

Step 2 From the **Protocol** drop-down list, select the AAA authentication and authorization method as per the following choices:

- *dot1x* — 802.1X Port-Based authentication helps prevent unauthorized client devices from gaining access to the network. It can be chosen only when a RADIUS authentication server has been configured and the network access switch can route packets to it.
- *mab* — MAC Authentication Bypass (MAB) uses the MAC address of the connecting device to grant or deny network access. The RADIUS server maintains a database of MAC addresses that require access. When this feature detects a new MAC address on a port, it generates a RADIUS request with both username and password as the device's MAC address. After authorization succeeds, the port is accessible to the particular device through the same code path.
- *web* — The web-based authentication feature, known as Web Authentication Proxy, enables you to authenticate end users on host systems that do not run the IEEE 802.1X supplicant.

  Note When configuring web-based authentication, note that fallback is configured on switch ports in access mode. Ports in trunk mode are not supported. Also, it is not supported on EtherChannels or EtherChannel members.

Step 3 From the **Server Group** drop-down list, select a server group host to associate it with this method.

Step 4 Select the interface from the **Interface List** and move it to the **Associated** column to associate it with the selected AAA authentication and authorization method.

Step 5 Click **Save & Apply to Device**.

Configuring ACL

Access Control List (ACL) performs packet filtering to control the movement of packets through a network. Packet filtering provides security by limiting the access of traffic into a network, restricting user and device access to a network, and preventing traffic from leaving a network. IP access lists reduce the chance of spoofing and denial-of-service attacks, and allow dynamic, temporary user-access through a firewall.

Creating ACLs

Step 1 On the **Services > ACL** page, click **Add**.

Step 2 Enter a name for the ACL.

Step 3 From the **ACL Type** drop-down list, choose the IP version to which the source or destination addresses belong.

Step 4 From the **Action** drop-down list, choose if you want to deny or permit traffic using this ACL.

Step 5 From the **Source Type** drop-down list, if you choose *Host*, enter the hostname to indicate the source address. If you choose *IP*, enter the source IP addressand subnet mask address. For IPv4 addresses, enter the subnet mask and for IPv6 addresses, enter the prefix length.

Step 6 (Only for IPv4 Extended and IPv6 source types) From the **Destination Type** drop-down list if you choose *Host*, enter the hostname to indicate the destination address. If you choose **IP**, enter the destination IP address. For IPv4 Extended addresses, enter the subnet mask and for IPv6 addresses, enter the prefix length.

Step 7 (Only for IPv4 Extended and IPv6 source types) From the **Protocol** drop-down list, choose the protocol you want to use for this ACL. The device can permit or deny only the IP packets in an ACL. Other types of packets (such as Address Resolution Protocol (ARP) packets) cannot be specified. This field is not available if your IP version is IPv4 Standard.

Step 8 Only for IPv4 Extended and IPv6 source types) If you chose TCP or UDP, two additional parameters, a source port and a destination port, are displayed. These parameters enable you to choose a specific source port and destination port or a port range. The port options are used by applications that send and receive data to and from the networking stack. Some ports are designated for specific applications such as Telnet, SSH, and HTTP.

Step 9 (Only for IPv4 Extended and IPv6 source types) To use the ACL to mark associated packets with a DSCP value, choose a value, from the **DSCP** drop-down list.

Step 10 Select the interfaces to be associated with this ACL and move them to the **Associated** column.

Step 11 Click **Save & Apply to Device** to apply your changes on the device.

Creating an ACE for an ACL

An Access Control Entry (ACE) consists of a series of ACL entries, which are permit or deny entries with criteria for the source IP address, destination IP address, protocol, port, or protocol-specific parameters. Each entry permits or denies inbound or outbound network traffic to the parts of your network specified in the entry.

You can use ACLs with the ACE to permit or deny traffic to or from a specific IP address or an entire network. For example, you can permit all e-mail traffic on a circuit, but block Telnet traffic. You can also use ACLs to allow one client to access a part of the network while preventing other clients from doing so.

Step 1 On the **Security > ACL > Access Control List** page, click the value in the ACE Count field. The Access Control List page for the selected ACL is displayed.

Step 2 Click **Add**. The Add ACE Setup window is displayed.

Step 3 In the **Sequence** field, type a sequence number for the ACE. An ACE sequence number is unique to an ACE and indicates the priority of an ACE within an ACL.

Step 4 From the **Action** drop-down list, choose if you want to deny or permit traffic using this ACE.

Step 5 From the **Source Type** drop-down list, if you choose Host, enter the hostname to indicate the source address.

Step 6 If you choose IP as the source type, enter the source IP address and the subnet mask.

Step 7 From the **Destination Type** drop-down list, choose the destination IP or host to indicate the destination address.

Step 8 Select the **Protocol** to be matched in the IP packet header. Any value matches any protocol in the IP header of the packet.

Step 9 Select the **DSCP** type to specify the specific DSCP values to match in the IP packet header.

Step 10 Click **Save & Apply to Device.**.

Configuring Energy Saver

Cisco EnergyWise is used to manage the energy usage of powered devices in a EnergyWise network. By default, EnergyWise is disabled on the domain member. However, when you add a switch to a Energywise domain, EnergyWise is enabled on the switch and its PoE ports.

Enabling EnergyWise

To enable EnergyWise with default configuration value, click the **Energywise Status** toggle button on the **Services > Energy Saver > Ports** page. You can also override the default configuration values by clicking **Configure a Energywise Domain** link and provide custom values.

Step 1 On the EnergyWise Domain window enter the domain name to which this member switch belongs. Note that for the domain-name and domain-password:

- You can enter alphanumeric characters and symbols such as #, (, $, !, and &.
- Do not enter an asterisk (*) or a space between the characters or symbols.

Step 2 Set the domain security mode.

- *ntp-shared-secret*—Sets a strong password with NTP. If the time between members varies ±30 seconds, the domain member drops events.
- *shared-secret*—Sets a strong password without NTP.

Step 3 Set the domain password to authenticate all communication in the domain and optionally select encryption if you want the password to be encrypted.

- (Optional) 0—Uses a plain-text password. This is the default.
- (Optional) 7—Uses a hidden password.
- If you do not enter 0 or 7, the default is 0.

Step 4 Enter the UDP port number to communicate with the EnergyWise domain.. The range is from 1 to 65000 and the default is 43440.

Step 5 From the **Interface/IP** drop-down list, if you select Interface, choose the interface from the list of available interfaces. Otherwise select IP from the drop-down list and enter the IP address that will be used to communicate with the domain server.

Step 6 Click **Save & Apply to Device** to apply your changes on the device.

Enabling Energy Efficient Ethernet (EEE)

Energy Efficient Ethernet (EEE) is an IEEE 802.3az standard that is designed to reduce power consumption in Ethernet networks during idle periods. EEE can be enabled on devices that support low power idle (LPI)

mode. EEE is enabled by default. If you need to disable EEE on all interfaces, click the **EEE Status** toggle button on the **Services > Energy Saver > Ports** page and click **Apply**. This disables EEE on all interfaces. Alternately, if you want to disable EEE on a particular interface, click on the green EEE icon. The green icon turns red is EEE is disabled on an interface.

Enabling Wake-on-LAN (WOL)

Wake-on-LAN (WoL) is an Ethernet computer networking standard, where you can use a network message to wake up a computer. You can send a WoL magic packet to a specific device in the EnergyWise network by clicking the green play icon on the **Services > Energy Saver > Ports** page. However, to do this, the EnergyWise status should be enabled. A red play icon indicates that there are no clients connected to this interface and therefore WoL is not applicable.

Configuring Power Level

EnergyWise uses a set of power levels to consistently manage power usage. A power level is a measure of the energy consumed by devices in an EnergyWise network.

To configure the power level on the Services > Energy Saver > Clients page, ensure that the EnergyWise Status is enabled.

Step 1 Click the Power level drop-down list and make a selection. The available values are:

Option	Description
Level	Description
10	Full
2	Sleep
1	Hibernate
0	Shutoff

Step 2 Click **Apply**. If you want the same power settings for all the devices in the EnergyWiise network, check the **Apply to all** checkbox and click **Apply**.

Configuring SPAN

You can analyze network traffic passing through ports or VLANs by using Switched Port Analyzer (SPAN) to send a copy of the traffic to another port on the switch. SPAN copies (or mirrors) traffic received or sent (or both) on source ports or source VLANs to a destination port for analysis. SPAN does not affect the switching of network traffic on the source ports or VLANs.

You can use the SPAN destination port to inject traffic from a network security device. For example, if you connect a Cisco Intrusion Detection System (IDS) sensor appliance to a destination port, the IDS device can send TCP reset packets to close down the TCP session of a suspected attacker.

Local SPAN: It supports a SPAN session entirely within one switch; all source ports or source VLANs and destination ports are in the same switch. Local SPAN copies traffic from one or more source ports in any VLAN or from one or more VLANs to a destination port for analysis.

Remote SPAN: Remote SPAN (RSPAN) is not supported on Cisco Catalyst 2960-L and Cisco Catalyst 2960-L Smart Managed Switches..

Creating a Local SPAN Session

Step 1 On the **Services > SPAN** page, click **Add**. A new **Create SPAN** window appears.

Step 2 From the **Source** drop-down list, choose *Local*.

Step 3 From the **Source Direction** drop-down list, choose one of the following:

- None
- Ingress
- Egress
- Both

Step 4 From the **Available** column, choose the ports you want into the **Selected** column.

Step 5 From the **Destination** drop-down list, choose *Local*.

Step 6 From the **Available** column, choose the ports you want into the **Selected** column.

Step 7 To enable traffic-filtering, choose the **Enable Filtering** check box and choose one of the following options:

- From the **Filter Type** drop-down list, choose *IPV4* and make a selection from the **Available ACLs** drop-down list.
- From the **Filter Type** drop-down list, choose *IPV6* and make a selection from the **Available ACLs** drop-down list.
- From the **Filter Type** drop-down list, choose **VLAN** and enter a value in the **VLAN ID** field.

Step 8 Choose the interfaces to be associated with this ACL and move them to the **Associated** column.

Step 9 Click **Save & Apply to Device** to apply your changes on the device.

Editing a Session

Step 1 On the **Services > SPAN** page, choose a session in the table and make changes to the **Create SPAN** window.

Step 2 Click **Update & Apply to Device** to apply your changes on the device.

Configuring Routing Protocol

Routing Information Protocol (RIP) is a commonly used routing protocol in small-to-medium TCP/IP networks. It uses broadcast UDP data packets to exchange routing information. It uses hop count as the metric to rate the value of different routes. The hop count is the number of devices that can be traversed in a route. It sends routing-update messages at regular intervals and when the network topology changes. It uses several timers that determine variables such as the frequency of routing updates, the length of time before a route becomes invalid, and other parameters that you can update to suit your inter-network needs.

The Cisco implementation of RIP Version 2 (RIPv2) supports plain text and message digest algorithm 5 (MD5) authentication, route summarization, classless inter-domain routing (CIDR), and variable-length subnet masks (VLSMs).

Configuring RIP

Step 1 On the **Services > Routing Protocol > RIP** page, click **Add**. A new **Create RIP** window appears.

Step 2 From the **Rip Version** radio buttons, choose either *Version1* or *Version2*.

Step 3 In the **Network Address** field, enter a value.

Step 4 In the **Neighbour** field, enter the network address of the neighbouring device.

Step 5 For setting advanced parameters, click the **Advanced** radio button.

a) Check the **No Autosummary** check box to disable automatic network number summarization.
b) Check the **Disable Split Horizon** check box to disable split horizon on the chosen interface.
c) Check the **Passive Interface** check box to suppress routing updates on the chosen interface.
d) Check the **Timers** check box to set timers for *Flush*, *Update*, *Invalid*, and *Holddown*.
e) For the **Distance** field, enter a value to set the administrative distance.
f) For the **Maximum Paths** drop-down list, choose the number of paths for forwarding packets.
g) Check the **Auth Key** check box to enter key-chain name for authentication control.

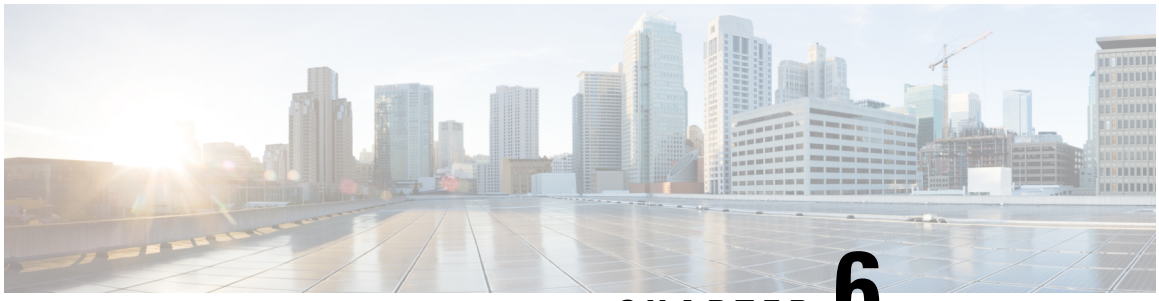
Step 6 Click **Save & Apply to Device** to apply your changes on the device.

Editing a Routing Protocol Setup

On the **Services > Routing Protocol > RIP** page, choose a setup in the table and make changes to the **Create RIP** window.

PART VI

General Settings



CHAPTER 6

Configuring General Settings

Configuring HTTPS Access

Certificate authorities (CAs) manage certificate requests and issue certificates to participating network devices. These services provide centralized security key and certificate management for the participating devices. Specific CA servers are referred to as trustpoints. When a connection attempt is made, the HTTPS server provides a secure connection by issuing a certified X.509v3 certificate, obtained from a specified CA trustpoint, to the client.

The client (usually a Web browser), in turn, has a public key that allows it to authenticate the certificate. For secure HTTP connections, we highly recommend that you configure a CA trustpoint. If a CA trustpoint is not configured for the device running the HTTPS server, the server certifies itself and generates the needed RSA key pair. Because a self-certified (self-signed) certificate does not provide adequate security, the connecting client generates a notification that the certificate is self-certified, and the user has the opportunity to accept or reject the connection. This option is useful for internal network topologies (such as testing). If you do not configure a CA trustpoint, when you enable a secure HTTP connection, either a temporary or a persistent self-signed certificate for the secure HTTP server (or client) is automatically generated.

If the device is not configured with a hostname and a domain name, a temporary self-signed certificate is generated. If the switch reboots, any temporary self-signed certificate is lost, and a new temporary new self-signed certificate is assigned. If the device has been configured with a host and domain name, a persistent self-signed certificate is generated. This certificate remains active if you reboot the device or if you disable the secure HTTP server so that it will be there the next time you re-enable a secure HTTP connection.

Step 1 Check the **HTTPS Access** check box to enable HTTPS on the device, and enter the designated port to listen for HTTPS requests. The default port is 1025. Valid values are 443, and ports between 1025 and 65535. On a secure HTTP connection, data to and from an HTTP server is encrypted before being sent over the Internet. HTTP with SSL encryption provides a secure connection to allow such functions as configuring a switch from a Web browser.

Step 2 In the **Trust Point Configuration** section, check the **Enable Trust Point** check box to use Certificate Authority servers as trustpoints.

Step 3 To keep track of hosts connecting to the device, check the **IP Device Tracking** check box.

Step 4 In the **Timeout Policy Configuration** section, enter the number of minutes of inactivity allowed before the session times out.

Step 5 Enter the server life time in seconds. Valid values can range from 1 to 86400 seconds.

Step 6 Enter the maximum number of requests the device can accept. Valid values range from 1 to 86400 requests.

Step 7 Click **Apply**.

Upgrading Device Software

Use the **General Settings > Software Upgrade** page to upgrade the software image on your device.

Step 1 Depending on whether you want to update only the WebUI image or the IOS bundle and WebUI image on your device, select the software from the **File Type** drop-down list.

Step 2 Browse to locate the file on your local device.

Step 3 Click **Start Update** to update the image.

Step 4 Click **Restart Switch** to boot your device after the device has been updated with the image.

Configuring System Settings

Setting Time Manually

Step 1 Choose **General Settings > System > Time > System Time**.

Step 2 In the **Set Date** and **Set Time** fields, set the date and the time for your device. This will override the time and date received from the NTP server (if configured).

Step 3 Choose the time zone associated with the location of the device.

Step 4 Coordinated Universal Time (UTC) is the 24-hour time standard and the basis for civil time today. Based on the time zone you selected, in the **Set Offset Hours** and **Set Offset Minutes** field, enter the number of hours and the number of minutes by which you want it offset from UTC, to arrive at your local time. For example, the offset for PST is -8 hours.

Step 5 Toggle to enable or disable **Daylight Savings Time**.

Step 6 Click **Apply** to save your changes. The system clock shows the device time and is refreshed every 30 seconds.

Setting Device Time Using NTP

A Network Time Protocol (NTP) network usually gets its time from an authoritative time source such as a radio clock or an atomic clock attached to a time server.

NTP then distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two machines to the accuracy of within a millisecond of one another. NTP uses the concept of a stratum to describe how many NTP hops away a machine is from an authoritative time source. A stratum 1 time server typically has an authoritative time source (such as a radio or atomic clock, or

a Global Positioning System (GPS) time source) directly attached, a stratum 2 time server receives its time via NTP from a stratum 1 time server, and so on.

Step 1 On the **General Settings > System > Time > NTP Server** page, click **Add**.

Step 2 Enter the Host name or the IP address of the server you want to add in the **Create NTP Server** window.

Step 3 Select the Interface to associate it with the NTP server. If you selected VLAN, select from the available list of VLANs. If you selected Interface , select the Interface from the drop-down list.

Step 4 Click **Save & Apply to Device**.

Transferring Configuration Files from the Device

Step 1 On the **General Settings > System > Config File** page, click **Add**.

Step 2 From the **Transfer** drop-down list, choose *From Switch*.

Step 3 From the **Src/Dest** drop-down list, choose either *TFTP* Server or a **Local Hard Drive** to indicate the location to which to transfer the configuration file.

Step 4 Type the name of the configuration file and provide the location of the file.

Step 5 If you choose TFTP server as the source, type the IP address of the server.

Step 6 Click **Apply**.

Transferring Configuration Files to the Device

Step 1 On the **General Settings > System > Config File** page, click **Add**.

Step 2 From the **Transfer** drop-down list, choose *To Switch*.

Step 3 From the **Src/Dest** drop-down list, choose either a TFTP server or a local directory to indicate the location from which to transfer the configuration file.

Step 4 Type the name of the configuration file and provide the location of the file.

Step 5 Enter the IP address of the TFTP server.

Step 6 Click **Apply**.

Creating DHCP Scopes

Network segments that do not have a separate DHCP server can have built-in DHCP scopes that assign IP addresses and subnet masks to hosts connecting to the device.

Step 1 Choose **General Settings > System > DHCP**.

Step 2 From the **DHCP Scopes** page, click Add. The **Create DHCP Scope** window is displayed.

Step 3 In the **Basic** section, enter a name for the new DHCP scope in the **DHCP Scope Name** field.

Step 4 In the **Network** field, enter the network served by this DHCP scope. This IP address is used by the management interface, as configured on the Interfaces page.

Step 5 In the **Subnet Mask** field, enter the subnet mask for the network.

Step 6 In the **Lease** fields, enter the amount of time that an IP address is granted to a client.

Step 7 In the **Default Router(s)** fields, type the IP address of the optional router or router(s) that connect to the device. Each router must include a DHCP forwarding agent that enables a single device to serve the clients of multiple devices.

Step 8 In the **Advanced** section, enter the IP address of the optional DNS server(s), in the **DNS Server(s)** field. Each DNS server must be able to update a client's DNS entry to match the IP address assigned by this DHCP scope.

Step 9 In the **NetBios Name Server(s)** field, enter the IP address of the optional Microsoft NetBIOS name servers, such as a Microsoft Windows Internet Naming Service (WINS) server.

Step 10 In the **Domain Name** field, enter the optional domain name of this DHCP scope for use with one or more DNS servers.

Step 11 To add DHCP options, click **Add**, in the **DHCP Options List** section. DHCP provides an internal framework for passing configuration parameters and other control information as DHCP options, to clients on your network. DHCP options carry parameters as tagged data stored within protocol messages exchanged between the DHCP server and its clients.

Step 12 Specify the DHCP option you want to add, and enter the option value.

Step 13 Click **Save**.

Configuring DHCP Excluded Addresses

Use the **General Settings > System > DHCP Excluded Address** section to specify IP addresses (excluded addresses) that the DHCP server should not assign to clients.

The IP address configured on the device interface is automatically excluded from the DHCP address pool. The DHCP server assumes that all other IP addresses in a DHCP address pool subnet are available to DHCP clients. If the DHCP server should not allocate some IP addresses to clients, add the IP addresses to the Excluded Addresses list. For example, if two DHCP servers are set up to service the same network segment (subnet) for redundancy. If the two servers do not coordinate their services with each other using a protocol such as DHCP failover, then each DHCP server must be configured to allocate from a non-overlapping set of addresses in the shared subnet.

Step 1 In the **DHCP Excluded Address** section, enter the IP address that you want to exclude, and the mask of the subnet to which the address belongs.

Step 2 Click **Apply**.

Creating Administrator Usernames and Passwords

You can configure administrator usernames and passwords to prevent unauthorized users from reconfiguring the switch and viewing configuration information.

Guidelines for Settings Passwords

- There should be at least three of the following categories—lowercase letters, uppercase letters, digits, and special characters.
- The new password should not be the same as the associated username or any close variant of the username.

- The characters in the password should not be repeated more than three times consecutively.
- The password should not be cisco, ocsic, admin, nimda, or any variant of the order of letters, or by substituting "1" "|" or "!" for i, and/or substituting "0" for "o", and/or substituting "$" for "s".
- The maximum number of characters accepted for the username and password is 32.

Creating a User Account

Step 1 On the **General Settings > User Administration** page, enter a user name for the new account.

Step 2 Specify the privilege level or you want to associate with the user. The privilege level defines what commands the user can enter using the CLI after they have logged into the device. Privilege 1 allows access in User Exec mode, privilege 15 allows access in Privileged Exec mode. To access the webUI, user should use highest privileged value i.e. 15.

Step 3 Enter a password with which to authenticate access to the device. Enter the password again to confirm it.

Step 4 Click **Done**.