Configuring the Device

- Configuring the Switch, on page 1
- Configuring Ports, on page 6
- Troubleshooting the Device, on page 11
- Configuring VLAN, on page 13

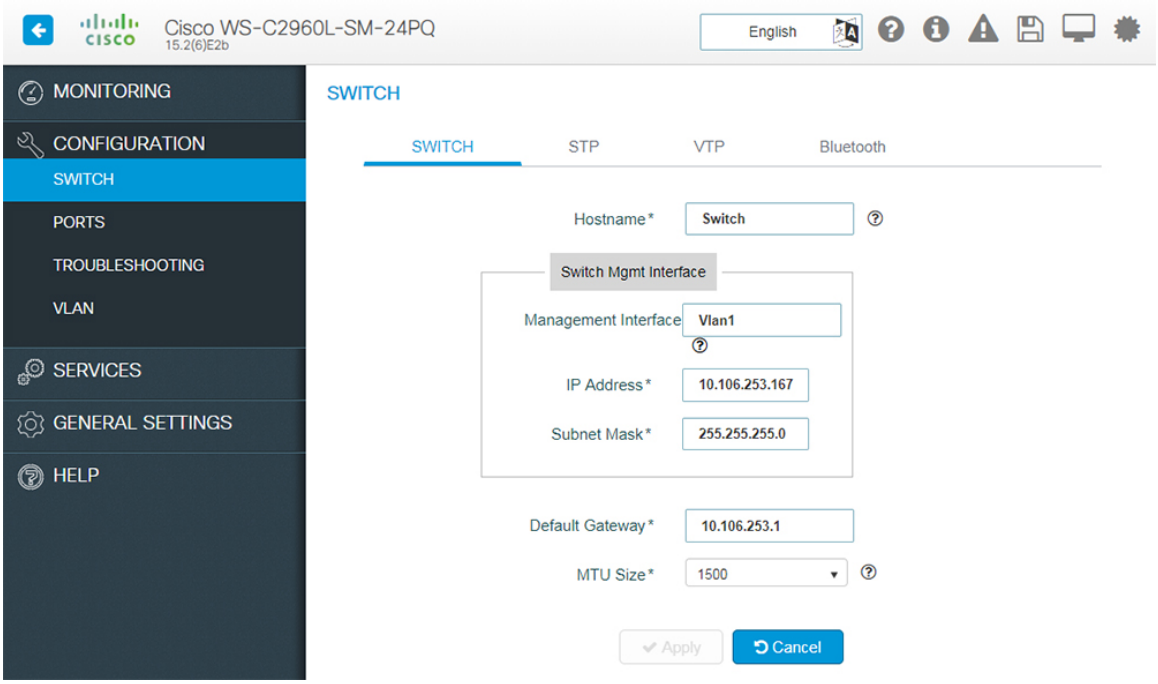
Configuring the Switch

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 1: 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.

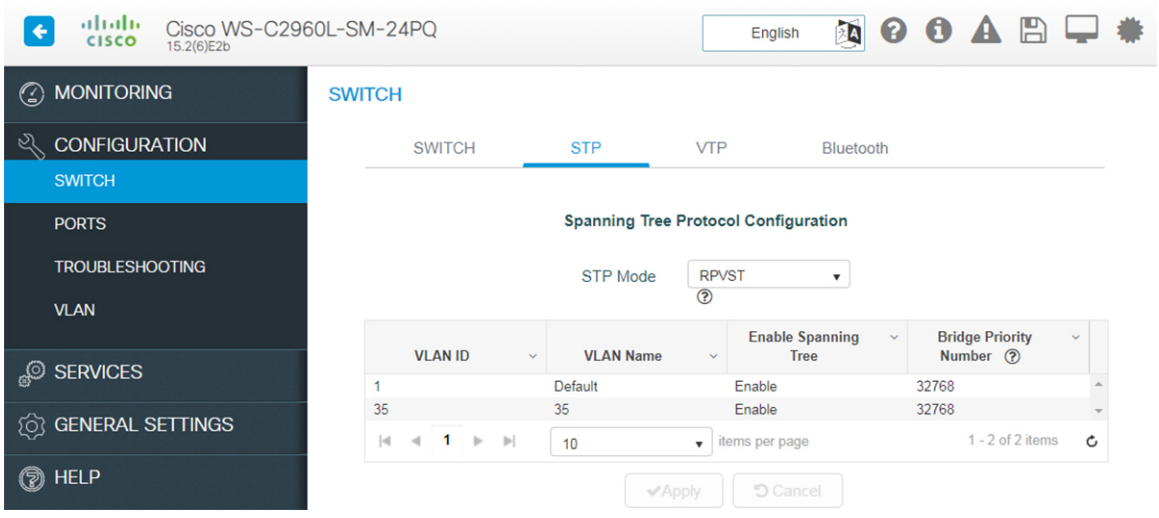
Step 5 Click **Apply** to save your changes.

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 2: 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.

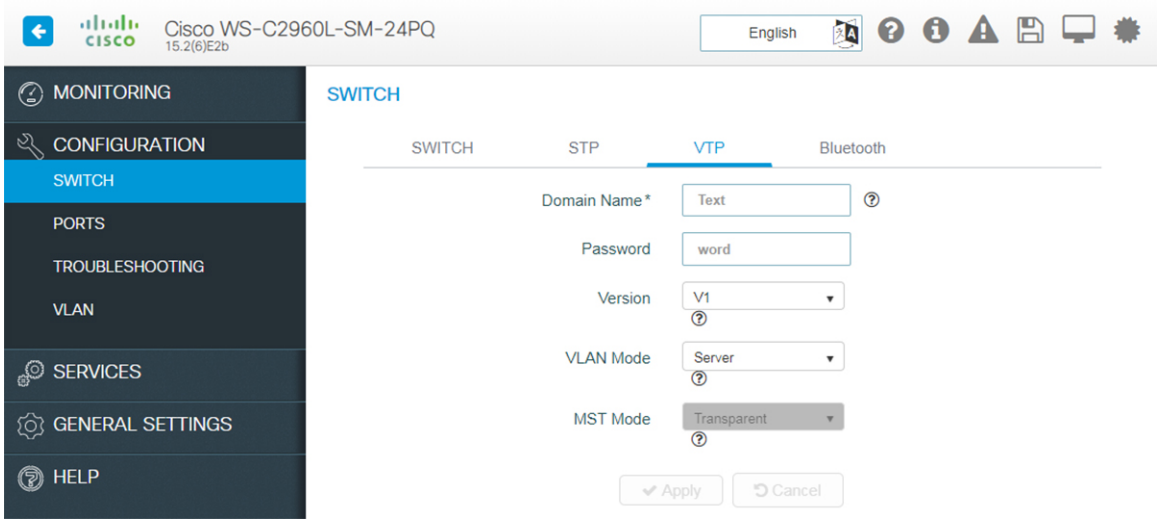
Step 9 Click **Apply**.

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 3: 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.

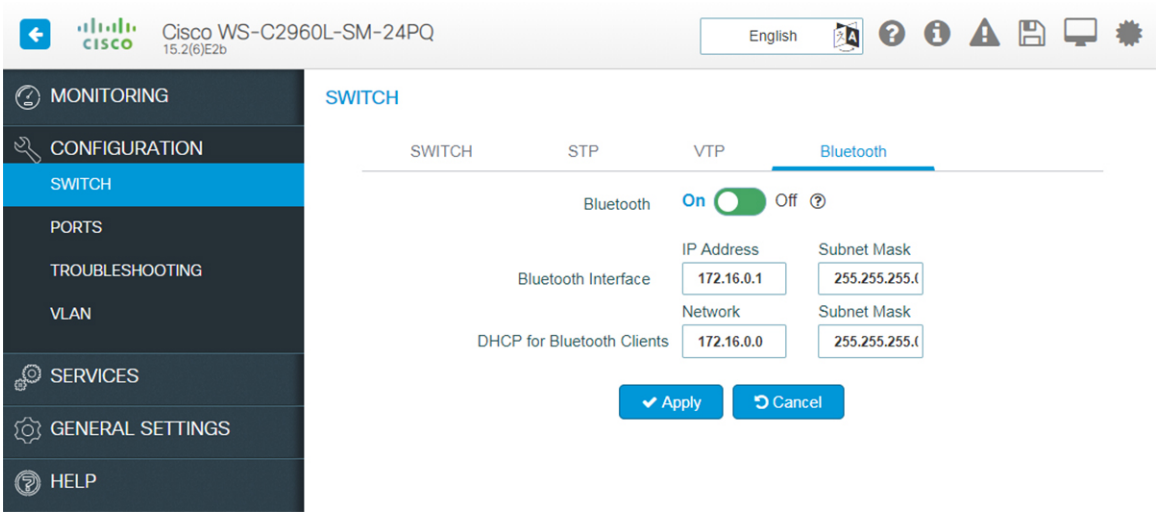
Step 7 Click **Apply** to save the changes.

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 4: 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

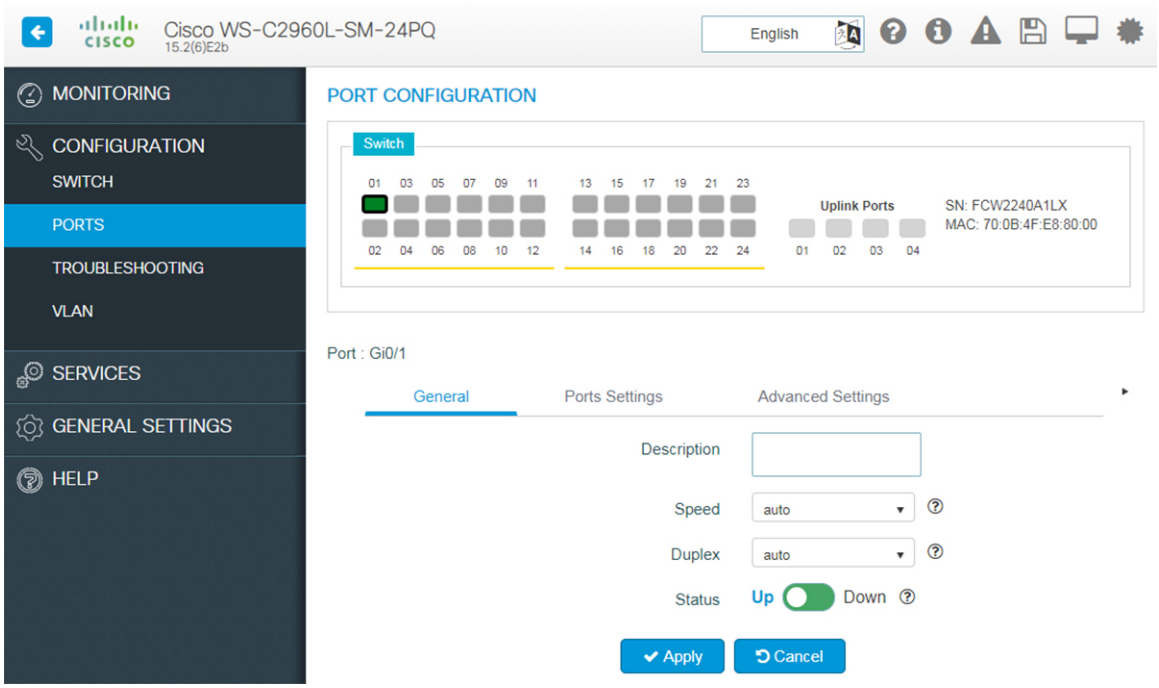
You can configure a port on the **Configuration > Ports > Port Configuration** page. By default, the first port is selected when you navigate to this page. You can select any other port by clicking on the switch view on the page. Additionally, you can view the port details by hovering over a port.

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 5: 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.

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.

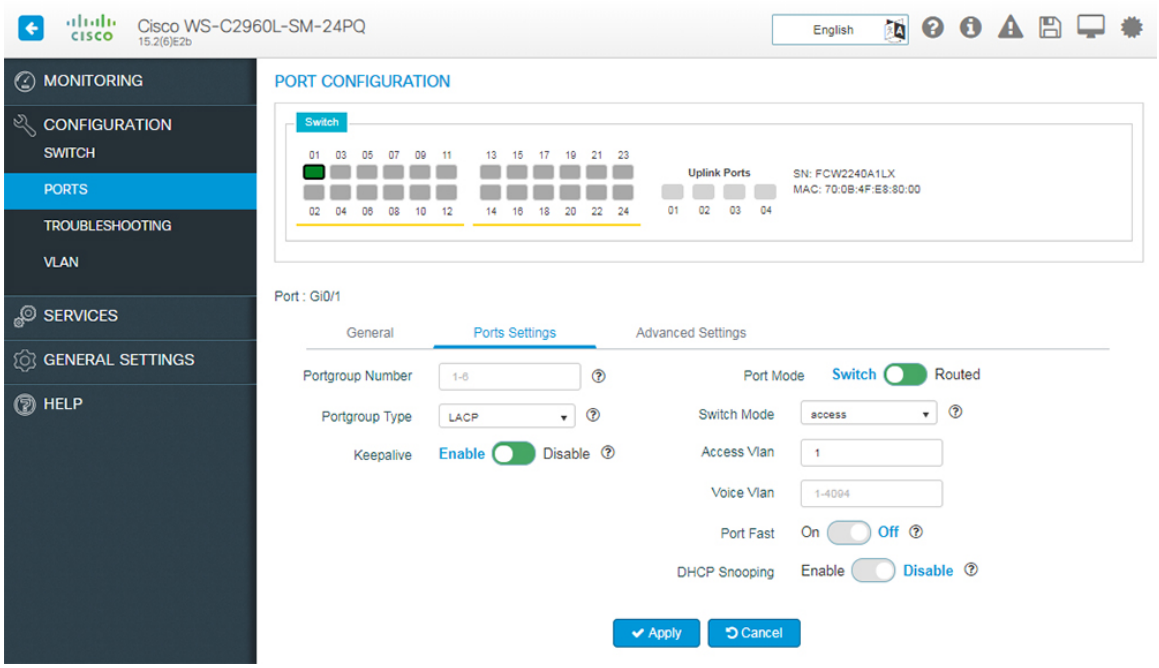
When you configure an EtherChannel in the On mode, no negotiations take place. The device forces all compatible ports to become active in the EtherChannel.

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 Click **Apply** to save your changes.

Configuring Port Settings - Layer 2 Interface

Figure 6: Configuring Port Settings



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:

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.

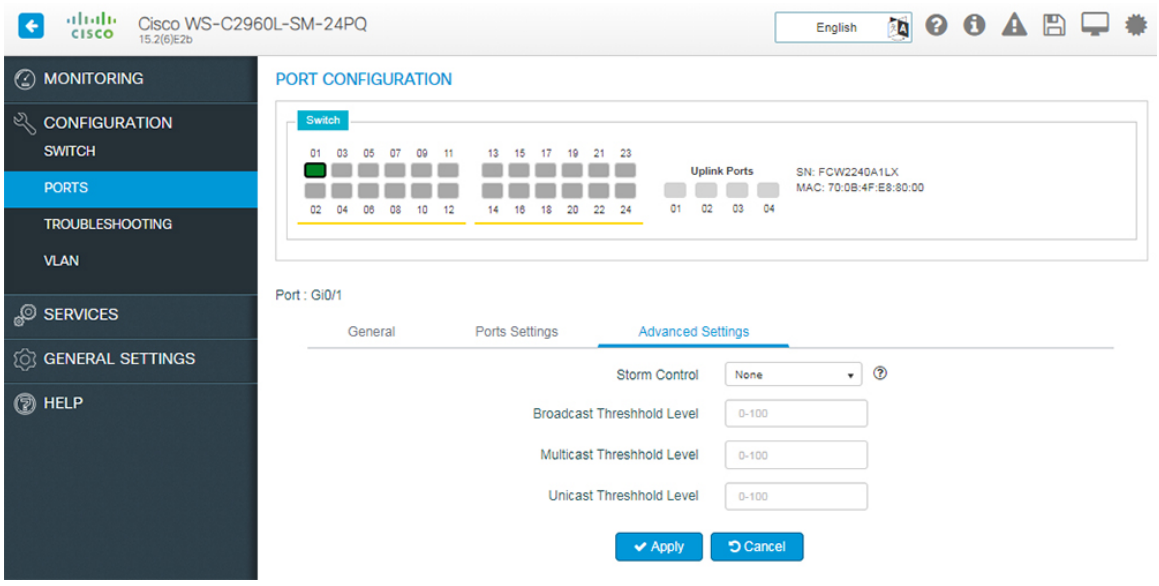
- To specify an IPv4 address and subnet mask for the interface, choose **Static IP**, from the **IP Type** drop-down list.
- To use DHCP to assign an IP address to the interface, choose **DHCP** from the **IP Type** drop-down list. Specify a hostname.
- To use an IP address from a DHCP pool, choose **DHCP Pool** from the drop-down list.

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 7: 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*.

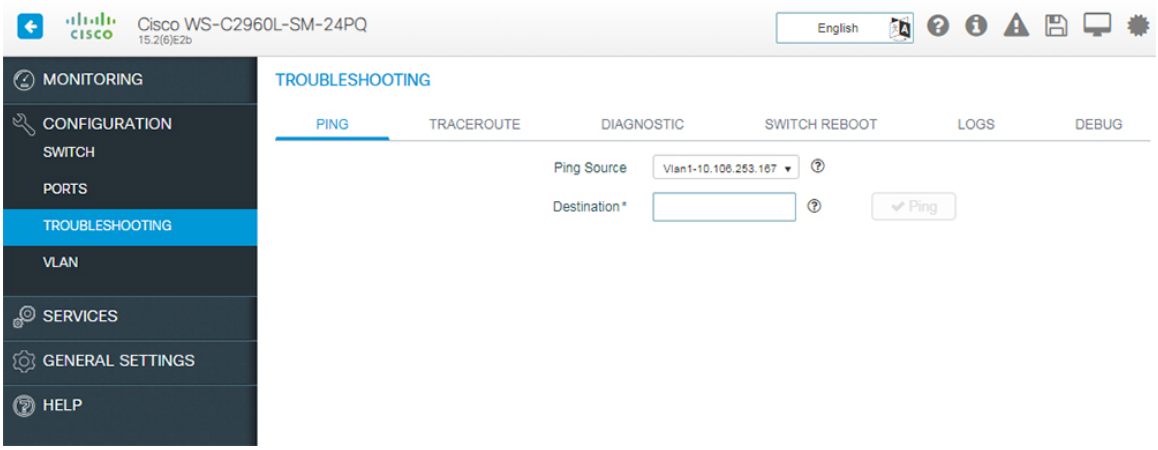
Step 3 Specify thresholds for unicast, broadcast, and multicast traffic entering your device. These values indicates the number of packets allowed per second, as part of your unicast, broadcast, and multicast traffic.

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 8: 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

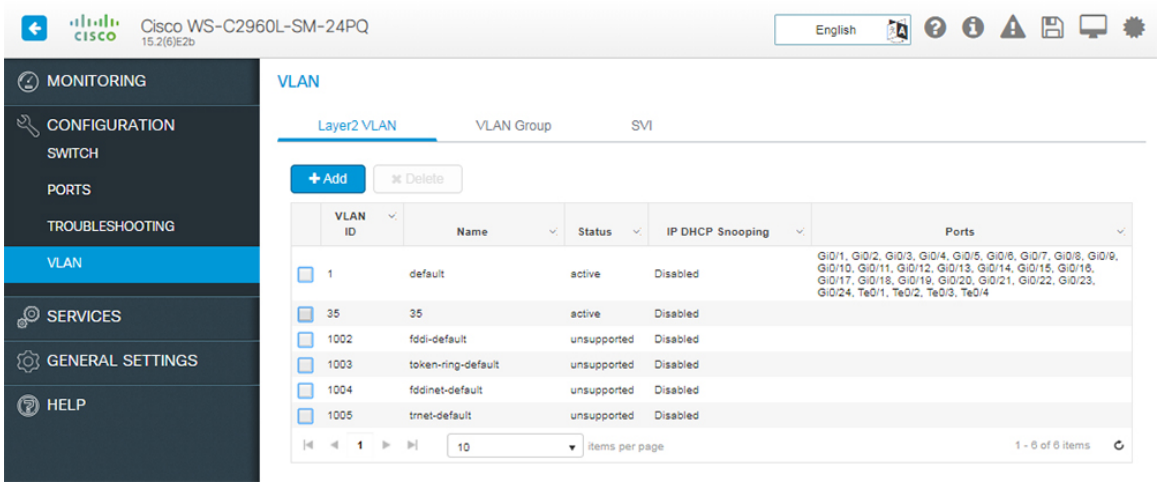
A VLAN or a virtual LAN is a group of devices on one or more LANs, which are configured to communicate as if they were physically connected, despite being located across LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

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 9: 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.

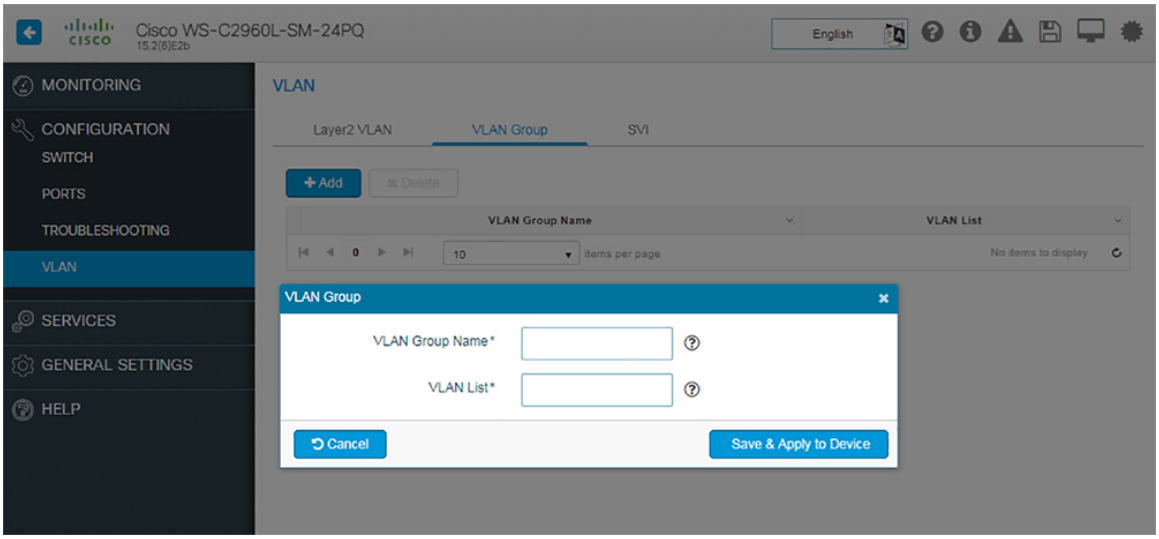
Step 4 Set the **State** toggle button to **Active** to forward traffic through the VLAN. VLANs in *suspended* state cannot forward traffic on your device.

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 10: Configuring VLAN Group



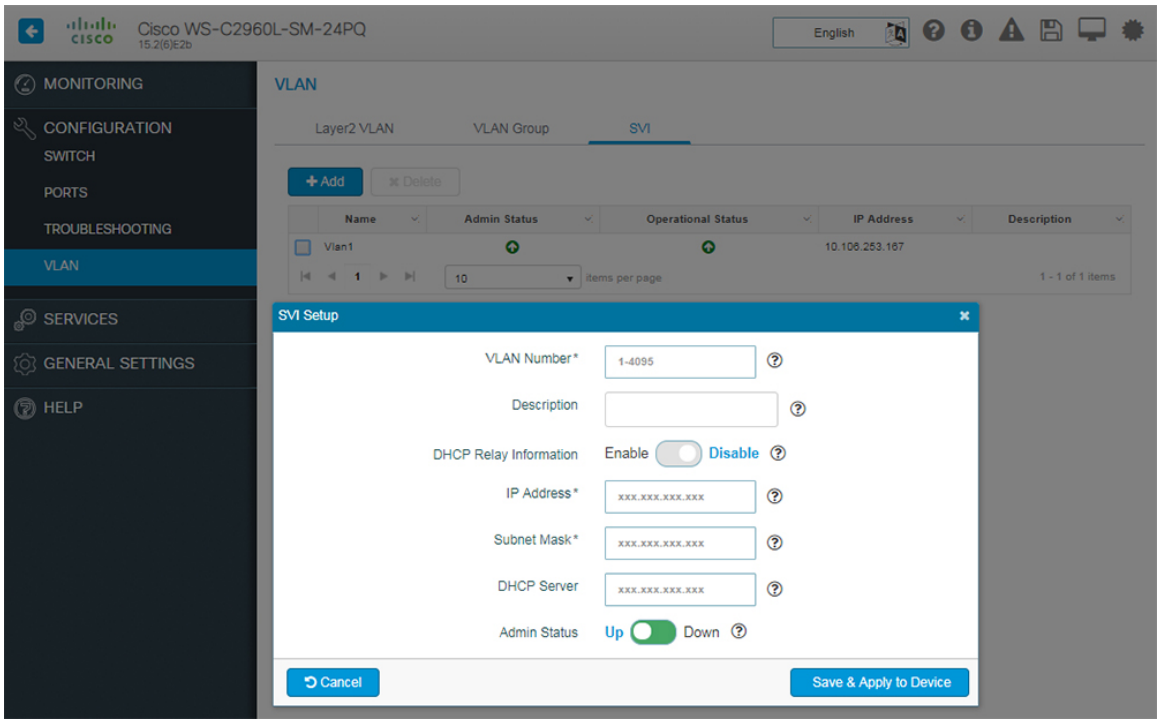
Step 1 On the **Configuration > VLAN > VLAN Group** page, click **Add** to create a VLAN Group. A VLAN group is a logical container for all the VLANs and ensures that the configured parameters are applicable to all the VLANs belonging to this group.

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 11: 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 IP Address and Subnet Mask.

Step 5 Enter the DHCP Server.

Step 6 Set **Admin Status** to **Enable**.

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