Configuring Your Device

- Configuring Access to the Device, page 1
- Configuring Stacking, page 2
- Configuring STP, page 2
- Configuring Device Ports, page 3
- Troubleshooting Your Device, page 5
- Rebooting Your Device, page 5
- Configuring VLANs, page 6
- Configuring Services, page 7

Configuring Access to the Device

**Step 1** Choose **Configuration > Switch > Switch**.

**Step 2** In the **Switch Host Name** field, enter a hostname to identify your device on the network. The hostname can be alphanumeric, is case sensitive, can contain special characters, and can have a maximum of 32 characters.

**Step 3** To be able to manage the switch remotely, assign an IP address in the **Switch IP Address** field.

**Step 4** Enter a VLAN ID to identify in the **Switch Management VLAN** field. The management VLAN is the VLAN that contains the interface that is used to remotely manage the switch. By default, this is VLAN 1, as all ports are assigned to VLAN 1. We recommend that you not use VLAN 1 or VLANs that are used by client devices such as users and printers.

**Step 5** Set the maximum transmission unit 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 MTU is 1500 bytes. Setting the MTU size sets the system MTU.

**Step 6** To control the Ethernet lights connected to your device, ensure that the **CoAP** checkbox remain selected. The connected Ethernet lights must support CoAP. By default, CoAP is already enabled on your device.

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

On the Configuration > Switch > Switch screen, on the Stacking tab, choose a value from the Stacking drop-down list to set your device as a standalone switch, as part of a physical stack, or as part of a cluster. The switch can belong to only one state at a time.

Step 1 To connect your switch to other switches on the stack ports, using a stacking cable, choose Physical Stacking. Click Apply.

Step 2 To enable clustering on your switch and allow your switch to start a cluster, choose Virtual Stacking. Click Apply. If your device is physically stacked, you cannot start a virtual cluster.

Step 3 To add a switch to the cluster, when Virtual Stacking is enabled, click Enable next to the switch MAC address. Enter the enable password of the cluster member, in the Enable Password field, to authenticate your action on the switch. Click OK.

Configuring STP

Understanding Spanning Tree Protocol

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

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 ports that are designated and that can communicate with the 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.

You device supports the following STP modes:

- RPVST
- PVST
- MST
## Configuring STP

**Step 1** Choose Configuration > Switch > STP.

**Step 2** From the STP Mode drop-down list, choose the STP mode for your device. Spanning-Tree Protocol (STP) prevents loops when switches are interconnected via multiple paths. STP implements the IEEE 802.1D algorithm by exchanging BPDU messages with other switches to detect loops, and then removes the loop by blocking selected bridge interfaces. This algorithm guarantees that there is only one active path between two network devices. Your device supports MST, PVST, and RPVST STP modes.

**Step 3** Ensure that STP is set to Enable for the interface.

**Step 4** Select a VLAN ID and update the bridge priority number. The bridge priority is a numerical value that is used with the MAC address, to find the switch on the network. The default value is 32768. The priority can only be configured in multiples of 4096.

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

## Configuring Device Ports

### Configuring Port General Settings

**Step 1** On the Configure > Ports > Port Configuration page. All the ports on your device are displayed. 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 Port Settings

Step 1  On the Configure > Ports > Port Configuration page. All the ports on your device are displayed. 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. For more information on Spanning Tree Protocol modes, see Understanding Spanning Tree Protocol, on page 2.

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 Advanced Port Settings

**Step 1**  On the Configuration > Ports > Port Configuration page. All the ports on your device are displayed. 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 indicate the number of packets allowed per second, as part of your unicast, broadcast, and multicast traffic.

**Step 4**  In the Policy Management section, choose an Auto-QoS policy to apply to the port. The Auto-QoS policy ensures that the traffic on the port receives the selected QoS treatment automatically.

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

Troubleshooting Your Device

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

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

On the Troubleshooting > Traceroute screen, 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.

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

Rebooting Your Device

Use the Troubleshooting > Switch Reboot screen, to restart your switch, and its stack members or restore it to factory defaults.

- **Restart Switch** - Click to reboot the switch. The switch restarts with your saved configuration.
- **Factory Reset** - Click to erase the startup configuration in the persistent memory on the switch and all its stack members, and reboot the switches with the initial factory default configuration. After you reset a switch, there is no way to recover the erased configuration.
Configuring VLANs

Understanding VLANs

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

Step 1  
On the Configure > VLANs page, click the Layer 2 VLANs page. 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 below.

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 description for the VLAN.

Step 4  
Set the State field to active to forward traffic through the VLAN. VLANs in suspended state cannot forward traffic on your device.

Step 5  
Click Apply to save your changes.

Configuring VLAN Groups

Step 1  
On the Configure > VLAN page, click the VLAN Groups tab. Click Add.

Step 2  
In the VLAN Group Name field, enter a name for the VLAN group that acts like a logical container for your VLANs. A VLAN group allows you to apply a set of common parameters to all the VLANs in the group.

Step 3  
In the VLAN List field, enter the range of VLANs, from 2 to 4094, you want to include in the VLAN group. The recommended number of VLANs in a group is 32.

Step 4  
Click Apply to save your changes.
Configuring DHCP Snooping on VLANs

Step 1  Choose Configuration > VLAN > IP DHCP Snooping.
Step 2  To activate DHCP snooping on a VLAN or a range of VLAN, set the IP DHCP Snooping field 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 3  In the VLAN List field, enter a VLAN ID or a range of VLAN IDs on which you want to enable DHCP snooping.
Step 4  Click Apply to save your changes.

Configuring Services

Configuring NetFlow

The Services > NetFlow screen is not displayed, if your device does not support NetFlow.

Step 1  Choose Services > Netflow.
Step 2  From the Netflow Template field, choose a pre-defined template to determine what information to monitor in your network traffic. You can choose to monitor application and server usage, network security vulnerabilities, and network capacity and bandwidth usage.
Step 3  In the Collector IP Address field, enter the IP address of the designated device on which the exported Netflow data is collected.
Step 4  In the Switch Export Address field, choose the IP address to identify the switch interface from which flows will be exported to the collector.
Step 5  From the Sampling Method field, choose the method based on which traffic originating from the port is monitored.
  • Deterministic – Monitors the first packet in a specified number of packets. For example, to monitor 1 in every 30 packets, specify 30 as the sampling method range.
  • Random – Allows packets to be monitored randomly by the device.
  • Full NetFlow – Monitors all the traffic on the specified device port. This option is not displayed if your device does not support Full NetFlow.
Step 6  In the Input Capture Interface drop-down list, choose the switch interface on which to apply NetFlow.
Step 7  Click Create to apply the NetFlow. The NetFlow Monitor section displays the flow monitor you created.