# Configuration Wizards

This chapter contains the following sections:


- Getting Started Wizard, on page 1
- VLAN Configuration Wizard, on page 3
- ACL Configuration Wizard, on page 3


## Getting Started Wizard

The Getting Started Wizard will assist you in the initial configuration of the device.

### Procedure

**Step 1** In **Configuration Wizards** > **Getting Started Wizard**, click **Launch Wizard.**

**Step 2** Click **Next** and enter the fields under General Information.

- System Location—Enter the physical location of the device.
- System Contact—Enter the name of a contact person.
- Host Name—Select the host name of this device. This is used in the prompt of CLI commands:
  - Use Default—The default hostname (System Name) of these switches is: switch 123456, where 123456 represents the last three bytes of the device MAC address in hex format.
  - User Defined—Enter the hostname. Use only letters, digits, and hyphens. Host names cannot begin or end with a hyphen. No other symbols, punctuation characters, or blank spaces are permitted (as specified in RFC1033, 1034, 1035).

**Step 3** Click **Next**.

**Step 4** Enter the fields in the IP Settings tab:

- Interface—Select from one of the following options for the IP interface.
  - Unit - Select the unit from the drop-down menu
  - Port - Select the port number from the drop-down menu.

- LAG - Enter the LAG
- VLAN - Enter the VLAN
- Loopback
- None

- IP Interface Source—Select one of the following options:
  - DHCP—Select for the device to receive its IP address from a DHCP server.
  - Static—Select to enter the IP address of the device manually.

- If you select DHCP complete the following
  - DNS Server - Enter the IP address of the DNS server.

- If you selected Static as the IP interface source, enter the following fields:
  - IP Address—IP address of the interface.
  - Network Mask—IP mask for this address.
  - Administrative Default Gateway—Enter the default gateway IP address.
  - DNS Server—Enter the IP address of the DNS server.

**Step 5** Click **Next**

**Step 6** Enter the fields in the User Account tab:

- Username—Enter a new user name between 0 and 20 characters. UTF-8 characters are not permitted.
- Password—Enter a password (UTF-8 characters are not permitted).
- Confirm Password—Enter the password again.
- Password Strength —Displays the strength of password.
- Keep current username and password—Select to keep current username and password.

**Step 7** Click **Next**

**Step 8** Enter the fields in the Time Settings tab:

- Clock Source—Select one of the following:
  - Manual Settings—Select to enter the device system time. If this is selected, enter the Date and Time.
  - Default SNTP Servers—Select to use the default SNTP servers.

**Note** The default SNTP servers are defined by name, thus DNS must be configured and operational.

- Manual SNTP Server—Select and enter the IP address of an SNTP server.

**Step 9** Click **Next** to view a summary of configuration that you entered.

**Step 10** Click **Apply** to save the configuration data.

# VLAN Configuration Wizard

The VLAN Configuration Wizard will assist you in configuring the VLANs. Each time you run this wizard, you can configure the port memberships in a single VLAN. To use the VLAN Configuration Wizard to configure your VLANs follow these steps:

### Procedure

**Step 1** In **Configuration Wizards** > **VLAN Configuration Wizard**, click **Launch Wizard**.

**Step 2** Click **Launch Wizard** and Next.

**Step 3** Select the ports that are to be configured as trunk port (by clicking with mouse on the required ports in the graphical display). Ports that are already configured as Trunk ports are pre-selected.

**Step 4** Click **Next**.

**Step 5** In the VLAN Configuration section, configure the following::

- VLAN ID—Select the VLAN you want to configure. You can select either an existing VLAN or New VLAN.
- New VLAN ID—Enter the VLAN ID of a new VLAN.
- VLAN Name—Optionally, enter VLAN name.

**Step 6** Select the trunk ports that are to be configured as untagged members of the VLAN (by clicking with mouse on the required ports in the graphical display). The trunk ports that are not selected in this step becomes tagged members of the VLAN.

**Step 7** Click **Next**.

**Step 8** Select the ports are that to be the access ports of the VLAN. Access ports of a VLAN is untagged member of the VLAN. (by clicking with mouse on the required ports in the graphical display).

**Step 9** Click **Next** to see the summary of the information that you entered.

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

# ACL Configuration Wizard

The ACL Configuration Wizard will assist you when creating a new ACL, or editing an existing ACL. To add or modify an existing ACL, complete the following steps:

### Procedure

**Step 1** In **Configuration Wizards** > **ACL Configuration Wizard**, click **Launch Wizard.**

**Step 2** Click **Next**.

**Step 3** In the ACL Configuration tab, select the ACL that you would like to configure from the drop-down menu. Then, enter the following fields:

- ACL Name—Enter the name of a new ACL.
- ACL Type—Select the type of ACL: IPv4 or MAC.

**Step 4** Click **Next**.

**Step 5** For the ACE Configuration, configure the following fields:

- Action on match—Select one of the options:
  - Permit Traffic—Forward packets that meet the ACL criteria.
  - Deny Traffic—Drop packets that meet the ACL criteria.
  - Shutdown Interface—Drop packets that meet the ACL criteria, and disable the port from where the packets received.

**Step 6** For a MAC-based ACL, enter the fields:

| | |
|---|---|
| Source MAC Address | Select Any if all source address are acceptable or User defined to enter a source address or range of source addresses. |
| Source MAC Value | Enter the MAC address to which the source MAC address is to be matched and its mask (if relevant). |
| Source MAC Wildcard Mask | Enter the mask to define a range of MAC addresses. |
| Destination MAC Address | Select Any if all destination addresses are acceptable or User defined to enter a destination address or a range of destination addresses. |
| Destination MAC Value | Enter the MAC address to which the destination MAC address is to be matched and its mask (if relevant). |
| Destination MAC Wildcard Mask | Enter the mask to define a range of MAC addresses. Note that this mask is different than in other uses, such as subnet mask. Here, setting a bit as 1 indicates don't care and 0 indicates to mask that value.<br>**Note**<br>Given a mask of 0000 0000 0000 0000 0000 0000 1111 1111 (which means that you match on the bits where there is 0 and don't match on the bits where there is 1's). You need to translate the 1's to a decimal integer and you write 0 for each four zeros. In this example since 1111 1111 = 255, the mask would be written: as 0.0.0.255. |
| Time Range Name | If Time Range is selected, select the time range to be used. |

**Step 7** For a IPv4-based ACL, enter the fields:

| | |
|---|---|
| Protocol | Select one of the following options to create an ACL based on a specific protocol:<br>• Any (IP)—Accept all IP protocols packets<br>• TCP—Accept Transmission Control Protocols packets<br>• UDP—Accept User Datagram Protocols packets<br>• ICMP—Accept ICMP Protocols packets<br>• IGMP—Accept IGMP Protocols packets |
| Source Port for TCP/UDP | Select a port from the drop-down list. |
| Destination Port for TCP/UDP | Select a port from the drop-down list. |
| Source IP Address | Select Any if all source address are acceptable or User defined to enter a source address or range of source addresses. |
| Source IP Value | Enter the IP address to which the source IP address is to be matched. |
| Source IP Wildcard Mask | Enter the mask to define a range of IP addresses. Note that this mask is different than in other uses, such as subnet mask. Here, setting a bit as 1 indicates don't care and 0 indicates to mask that value. |
| Destination IP Address | Select Any if all IP address are acceptable or User defined to enter a destination IP address or range of destination IP addresses. |
| Destination IP Value | Enter the IP value to which the destination IP value is to be matched. |
| Destination IP Wildcard Mask | Enter the mask to define a range of IP addresses. Note that this mask is different than in other uses, such as subnet mask. Here, setting a bit as 1 indicates don't care and 0 indicates to mask that value. |
| Time Range Name | If Time Range is selected, select the time range to be used. |

**Step 8** Click **Next**.

**Step 9** Confirm that you want the ACL and ACE to be created.

The details of the ACL rule are displayed. You can click **Add another rule to this ACL** to add another rule.

**Step 10** Click **Next** and enter the ACL Binding information:

- Binding Type—Select one of the following options to bind the ACL:
  - Physical interfaces only—Bind the ACL to a port. In this case, click a port or ports on which to bind the ACL.
  - VLANs only—Bind the ACL to a VLAN. Enter the list of VLANs in the Enter the list of VLANs you want to bind the ACL to field.
  - No binding—Do not bind the ACL.

Click **Apply**. A message will appear showing that the changes were applied successfully.

**Note** If the changes are not successful, the following pop-up message will appear: *Cannot bind ACL/policy map to an interface when DoS Prevention is enabled in per-port mode*.