Create VLANs on a Cisco Business 250 or 350 Switch

Objective

This article aims to show how to create, edit, or delete a VLAN on a Cisco Business 250 or 350 series switch.

Applicable Devices | Software Version

- CBS250 **(DataSheet)** | 3.0.0.69 **(Download latest)**
- CBS350 **(Data Sheet)** | 3.0.0.69 **(Download latest)**
- CBS350-2X **(Data Sheet)** | 3.0.0.69 **(Download latest)**
- CBS350-4X **(Data Sheet)** | 3.0.0.69 **(Download latest)**

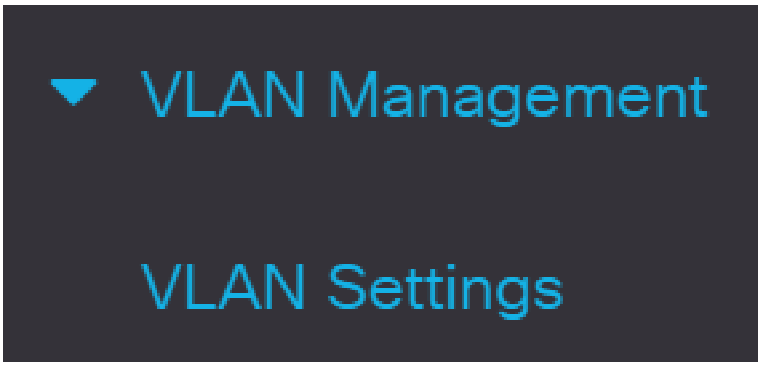
Introduction

Virtual Local Area Network (VLAN) creation allows you to make separate broadcast domains on a switch. The broadcast domains can associate with one another with the help of a Layer 3 device such as a router. A VLAN is mainly used to form groups among the hosts regardless of where the hosts are physically located. Thus, a VLAN improves security with the help of group formation among the hosts. When a VLAN is created, it has no effect until that VLAN is attached to at least one port either manually or dynamically. One of the most common reasons to set up a VLAN is to set up a separate VLAN for voice, and a separate VLAN for data. This directs the packets for both types of data despite using the same network.

VLAN Settings

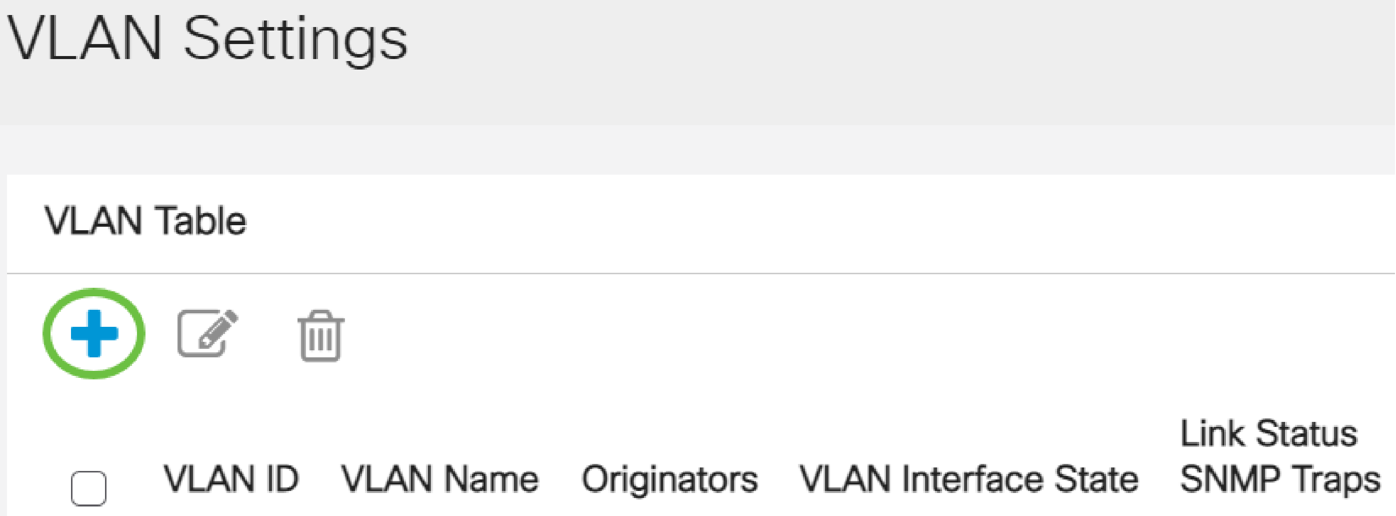
Create a VLAN

Step 1. Log in to the web-based utility and choose **VLAN Management > VLAN Settings**.



Step 2. Under the VLAN Table area, click Add to create a new VLAN. A window will

pop-up.

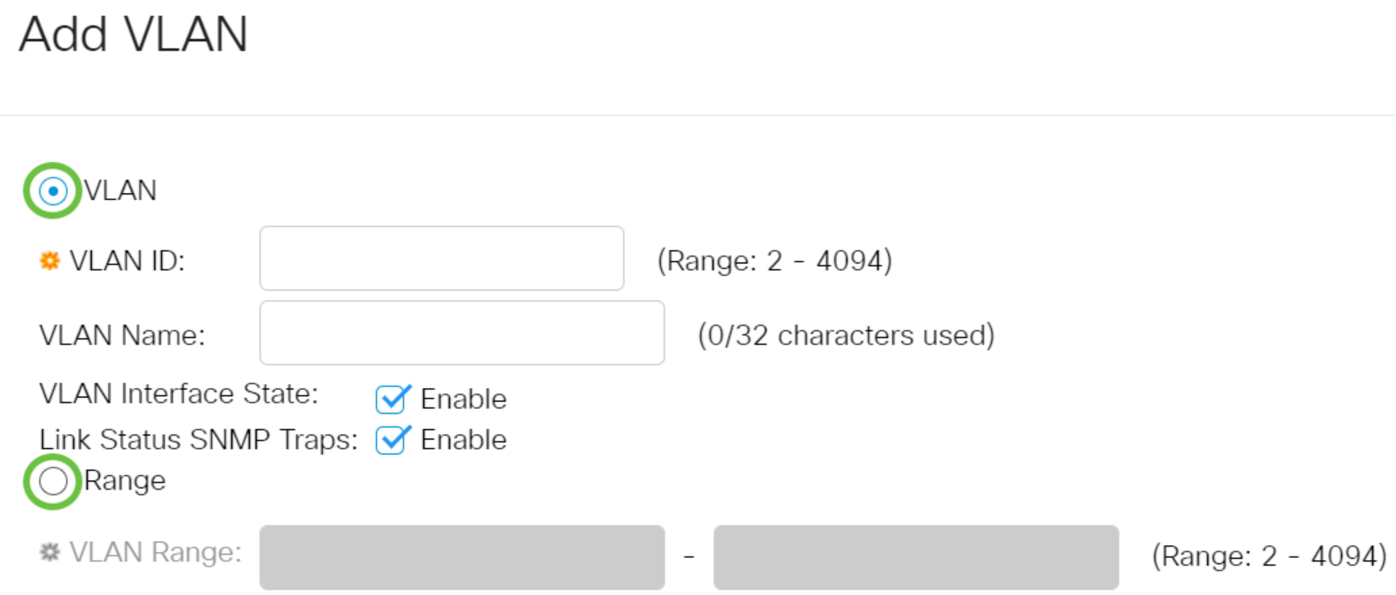


VLAN Settings

VLAN Table

□	VLAN ID	VLAN Name	Originators	VLAN Interface State	Link Status SNMP Traps

Step 3. VLAN can be added in two different methods as shown by the options below. Choose a radio button that corresponds to the desired method:



Add VLAN

● VLAN

VLAN ID: (Range: 2 - 4094)

VLAN Name: (0/32 characters used)

VLAN Interface State: ☑ Enable

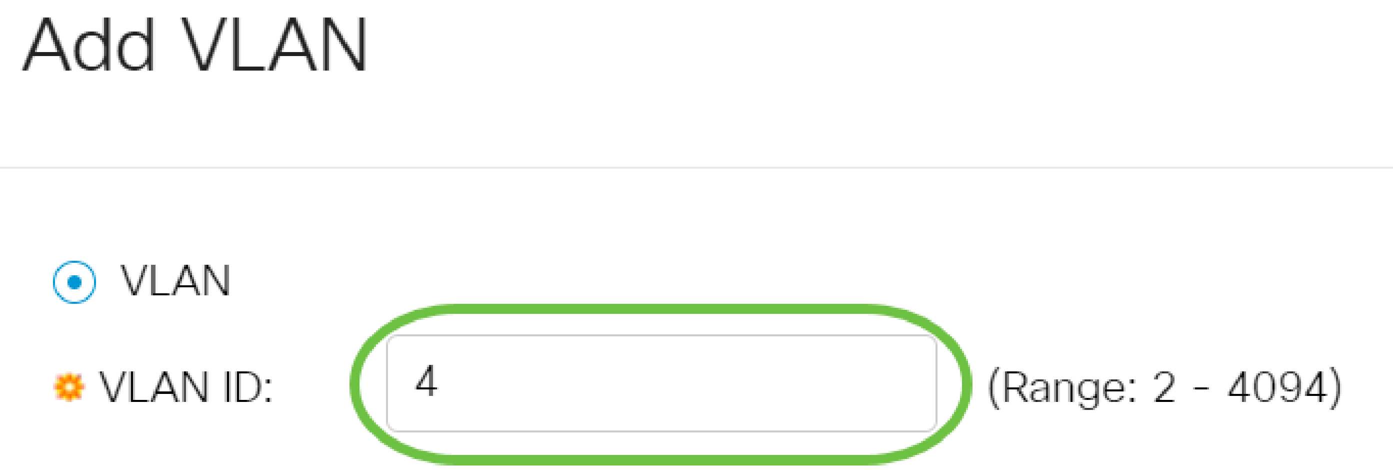
Link Status SNMP Traps: ☑ Enable

○ Range

VLAN Range: - (Range: 2 - 4094)

- VLAN - Use this method to create a specific VLAN.
- Range - Use this method to create a range VLANs.

Step 4. If you chose VLAN in Step 3, enter the VLAN ID in the VLAN ID field. The range must be between 2 to 4094. For this example, the VLAN ID will be 4.

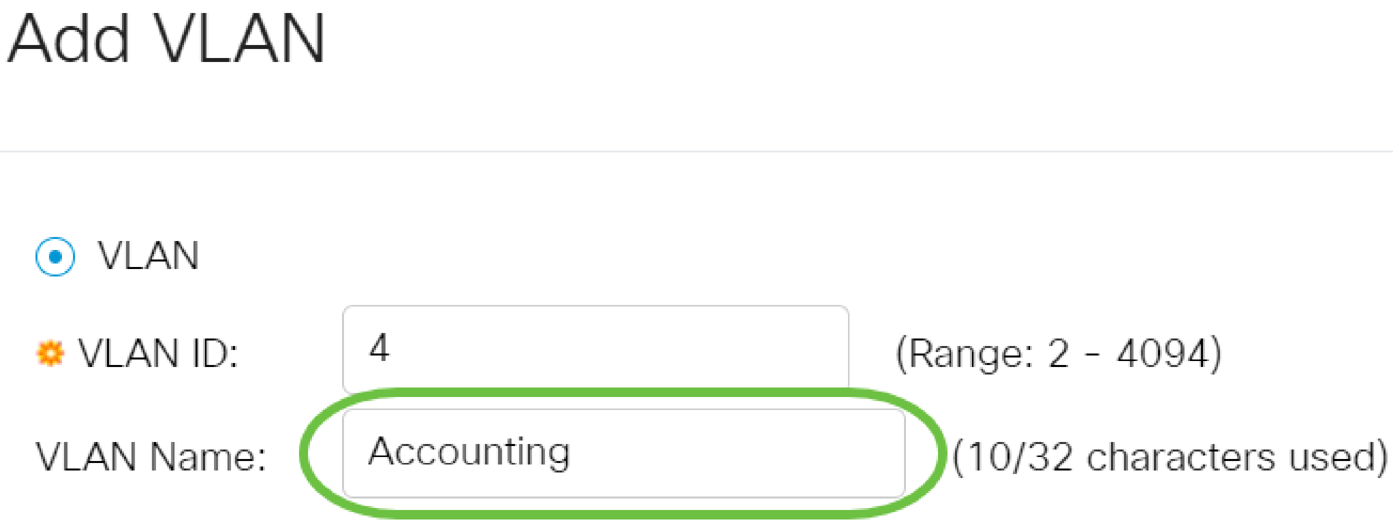


Add VLAN

● VLAN

VLAN ID: 4 (Range: 2 - 4094)

Step 5. In the *VLAN Name* field, enter a name for the VLAN. For this example, the VLAN Name will be Accounting. Up to 32 characters may be used.



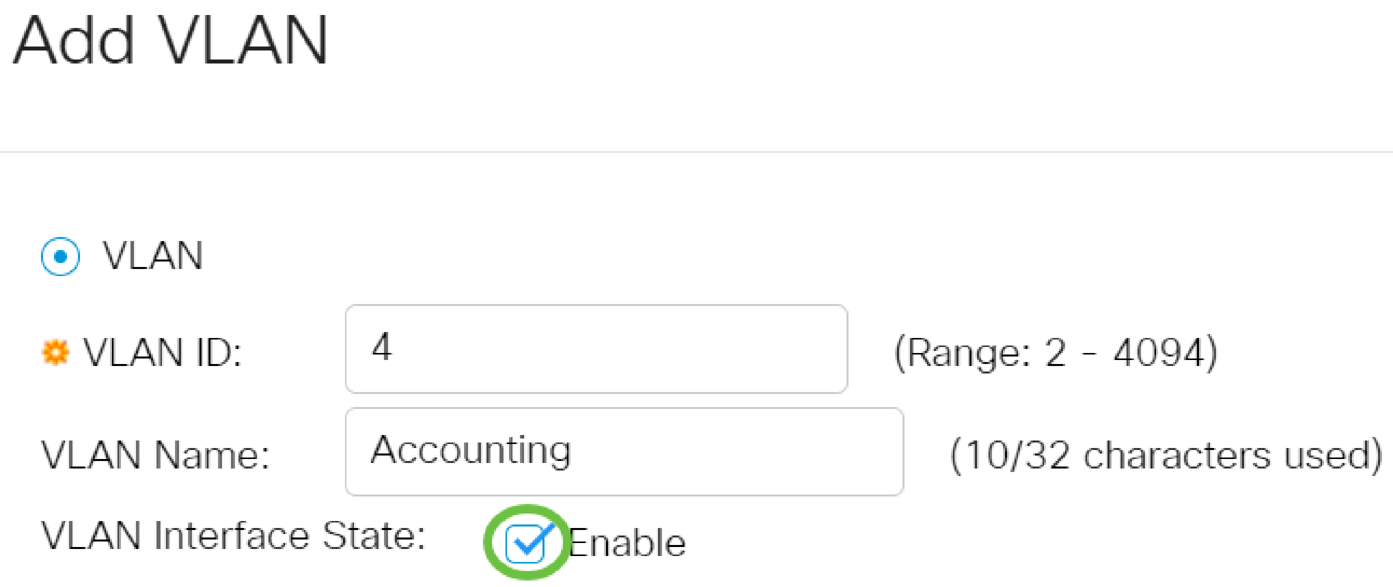
Add VLAN

● VLAN

VLAN ID: 4 (Range: 2 - 4094)

VLAN Name: Accounting (10/32 characters used)

Step 6. Check the *VLAN Interface State* check box to enable the VLAN interface state; it is already checked by default. If not, the VLAN will be effectively shut down, and nothing will be able to be transmitted or received through the VLAN.



Add VLAN

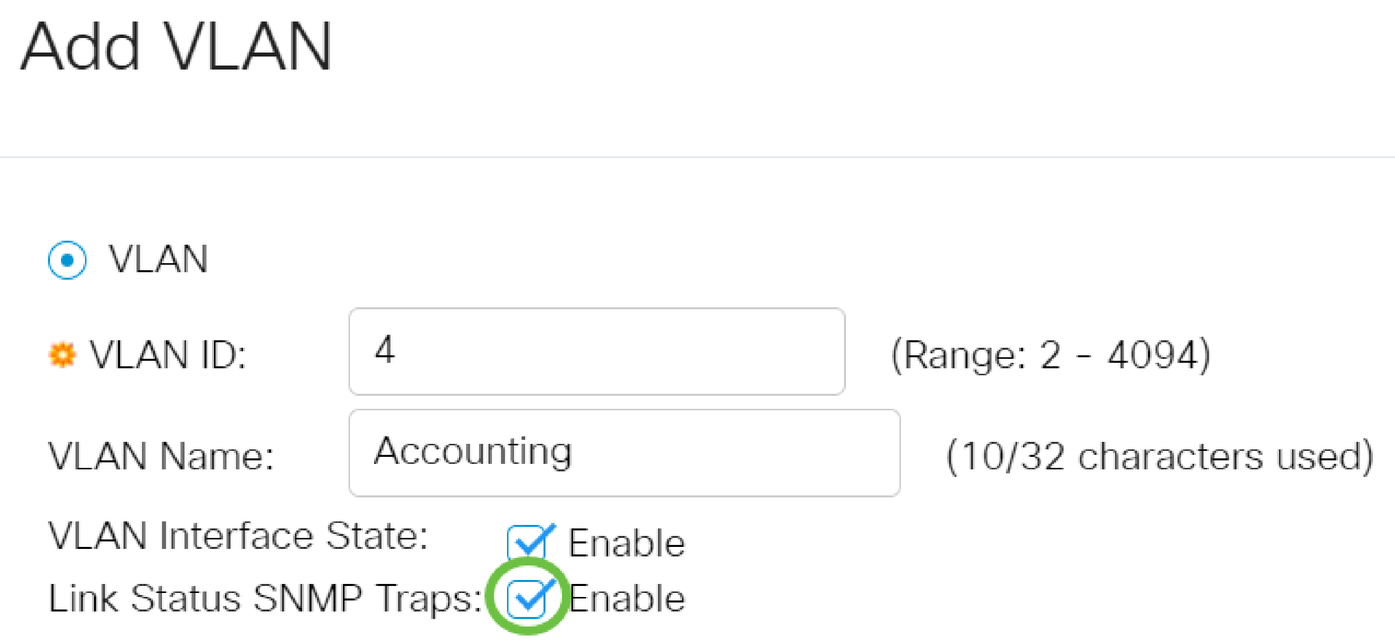
● VLAN

VLAN ID: 4 (Range: 2 - 4094)

VLAN Name: Accounting (10/32 characters used)

VLAN Interface State: ☑ Enable

Step 7. Check the Link Status SNMP Traps check box if you want to enable the generation of SNMP traps. This is enabled by default.



Add VLAN

● VLAN

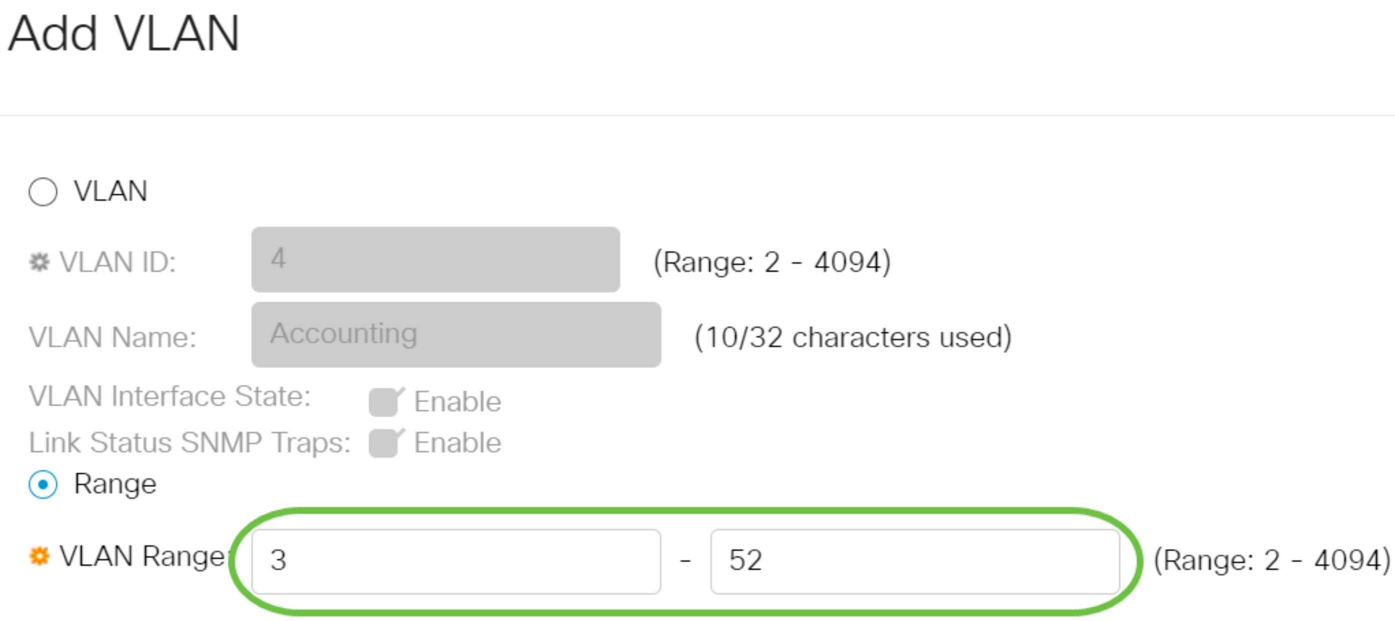
VLAN ID: 4 (Range: 2 - 4094)

VLAN Name: Accounting (10/32 characters used)

VLAN Interface State: ☑ Enable

Link Status SNMP Traps: ☑ Enable

Step 8. If you chose Range in Step 3, enter the range of the VLANs in the VLAN Range field. The available range is 2–4094. For this example, the VLAN Range is from 3 to 52.



Add VLAN

○ VLAN

VLAN ID: 4 (Range: 2 - 4094)

VLAN Name: Accounting (10/32 characters used)

VLAN Interface State: ☑ Enable

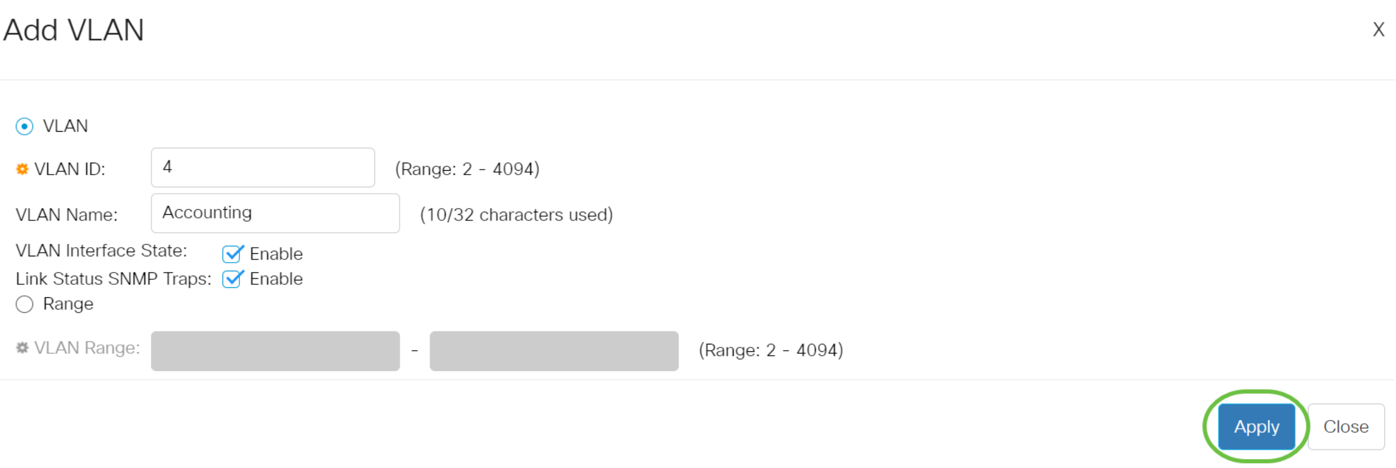
Link Status SNMP Traps: ☑ Enable

● Range

VLAN Range 3 - 52 (Range: 2 - 4094)

Up to 100 VLANs can be created at a time.

Step 9. Click Apply.



Add VLAN

● VLAN

VLAN ID: 4 (Range: 2 - 4094)

VLAN Name: Accounting (10/32 characters used)

VLAN Interface State: ☑ Enable

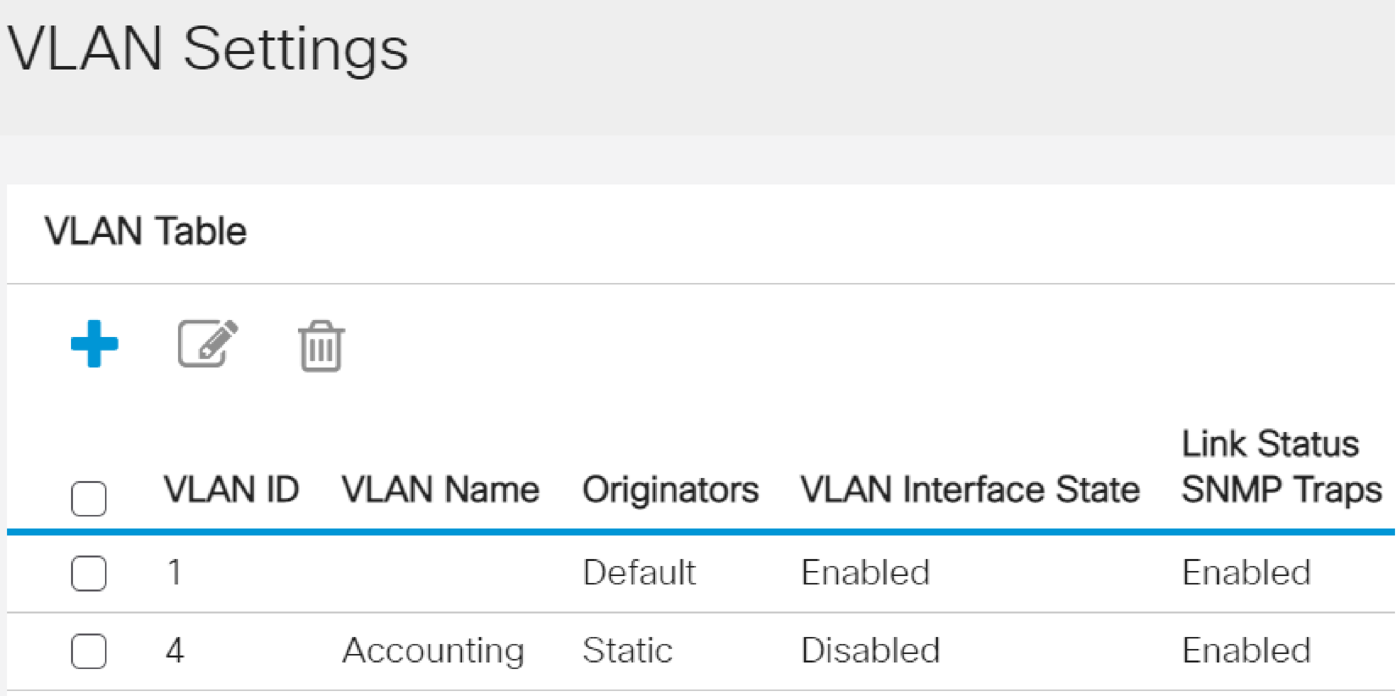
Link Status SNMP Traps: ☑ Enable

○ Range

VLAN Range: - (Range: 2 - 4094)

Edit a VLAN

Step 1. Log in to the web-based utility and choose **VLAN Management > VLAN Settings**. The *VLAN Settings* page opens.

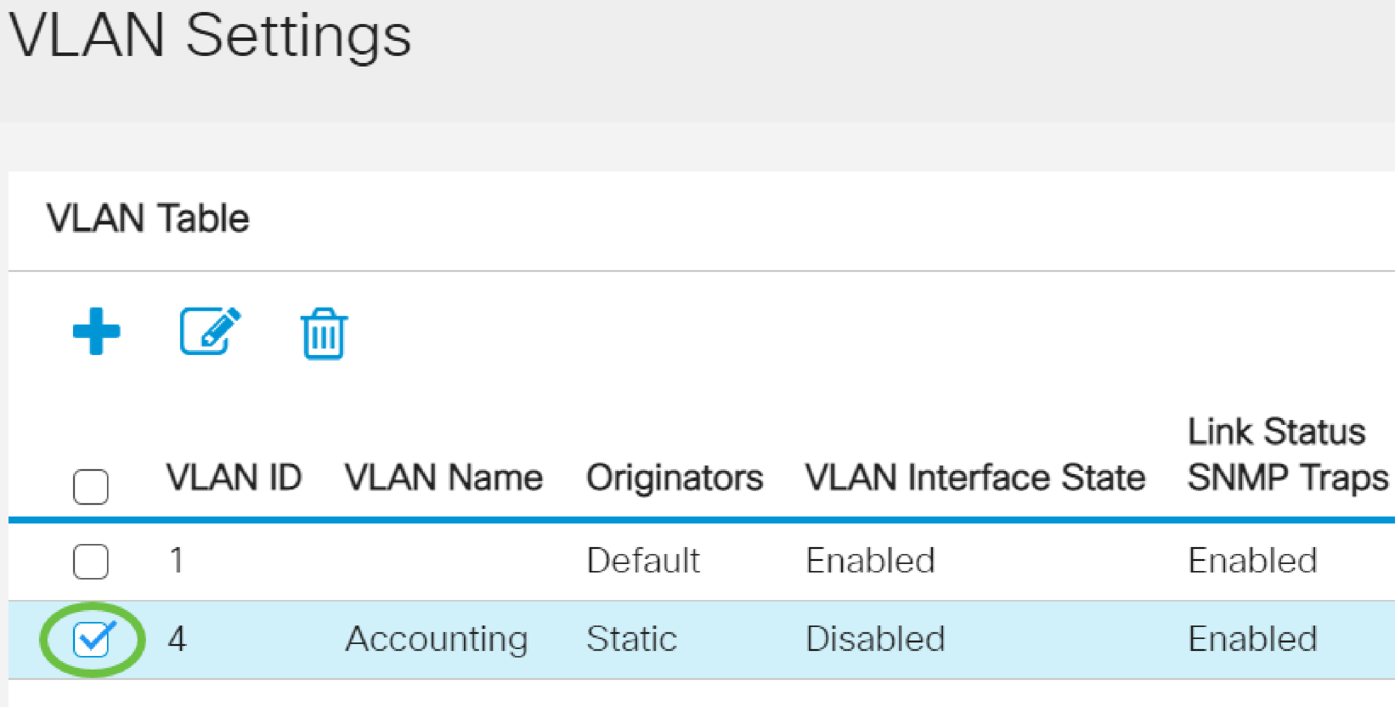


VLAN Settings

VLAN Table

□	VLAN ID	VLAN Name	Originators	VLAN Interface State	Link Status SNMP Traps
□	1		Default	Enabled	Enabled
□	4	Accounting	Static	Disabled	Enabled

Step 2. Check the check box next to the VLAN you want to edit.

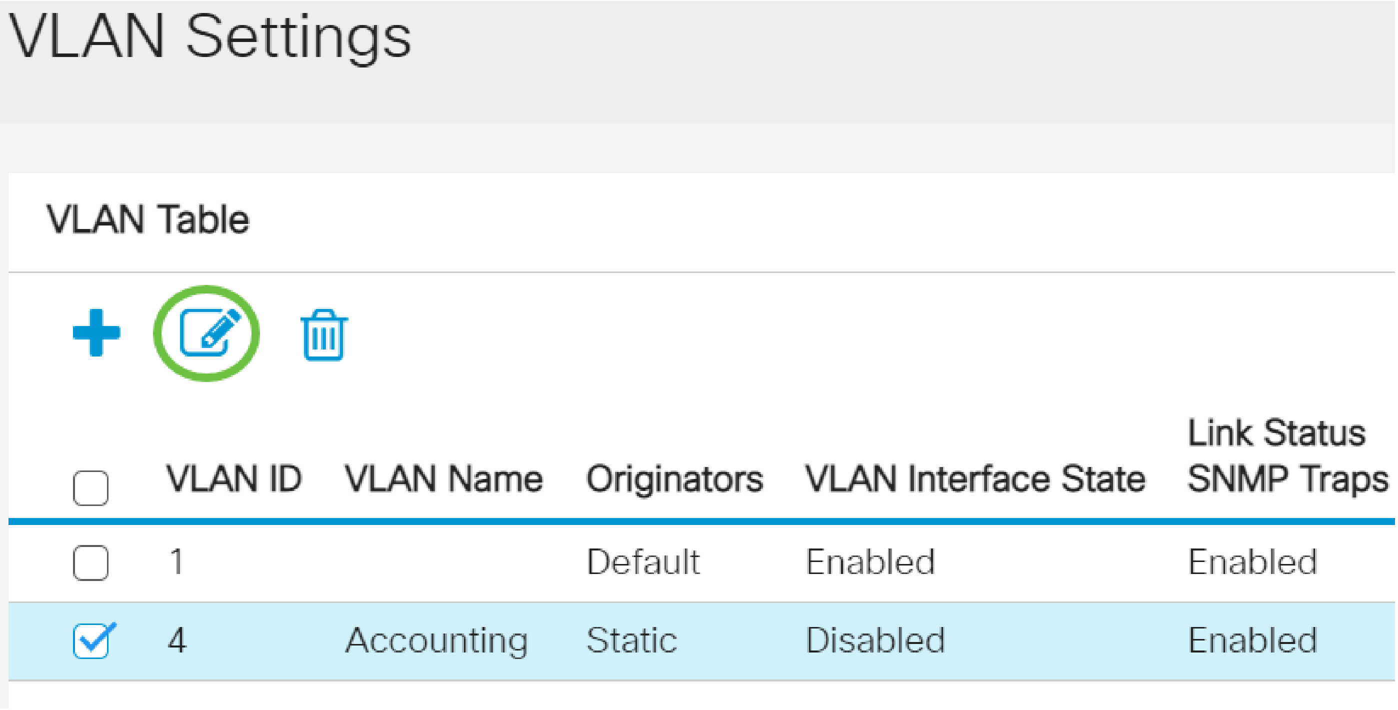


VLAN Settings

VLAN Table

□	VLAN ID	VLAN Name	Originators	VLAN Interface State	Link Status SNMP Traps
□	1		Default	Enabled	Enabled
☑	4	Accounting	Static	Disabled	Enabled

Step 3. Click **Edit** to edit the selected VLAN. The *Edit VLAN* window appears.

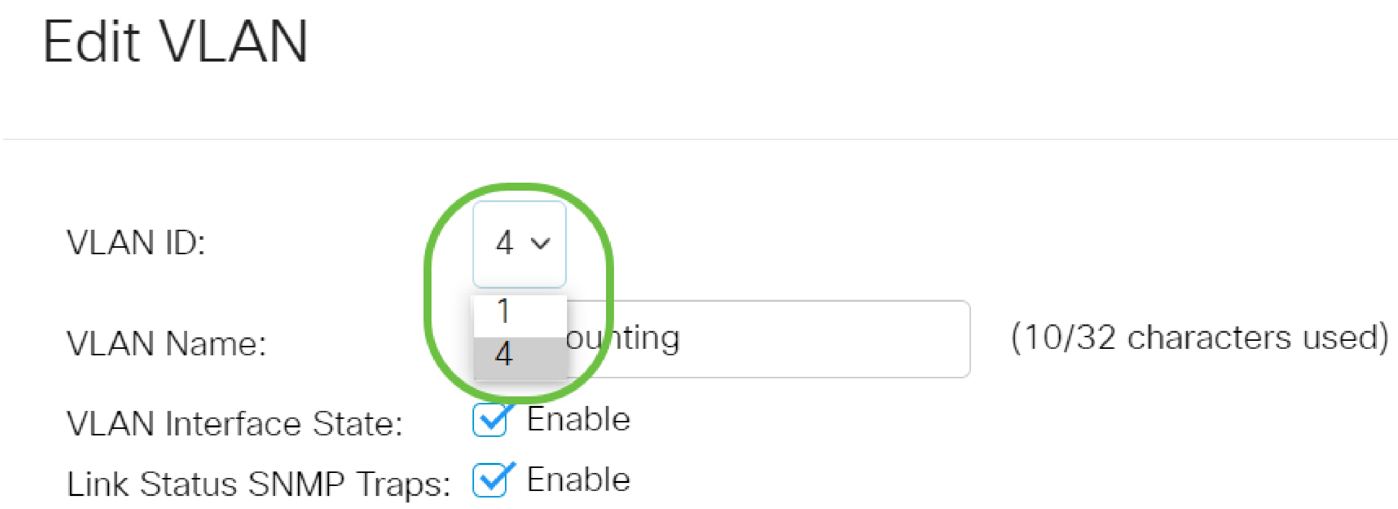


VLAN Settings

VLAN Table

□	VLAN ID	VLAN Name	Originators	VLAN Interface State	Link Status SNMP Traps
□	1		Default	Enabled	Enabled
☑	4	Accounting	Static	Disabled	Enabled

Step 4. The current VLAN can be changed using the *VLAN ID* drop-down list. This is used to quickly switch between the VLANs you want to configure without returning to the VLAN Settings page.



Edit VLAN

VLAN ID: 4

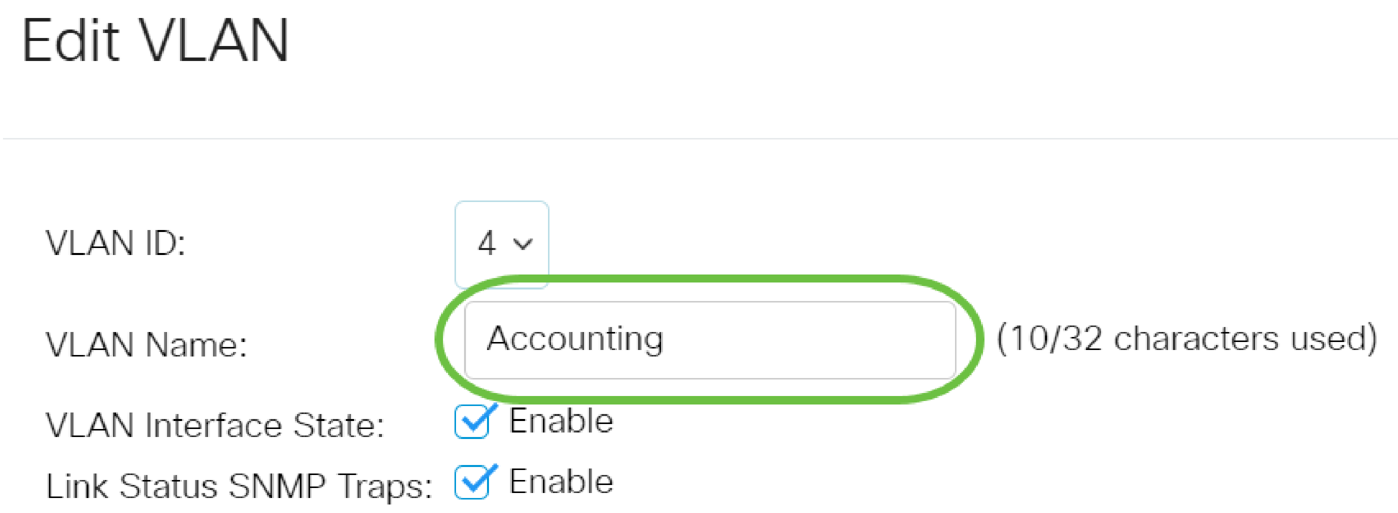
1
4

VLAN Name: ounting (10/32 characters used)

VLAN Interface State: ☑ Enable

Link Status SNMP Traps: ☑ Enable

Step 5. Edit the name of the VLAN in the *VLAN Name* field. This name does not impact the performance of the VLAN, and is used for easy identification.



Edit VLAN

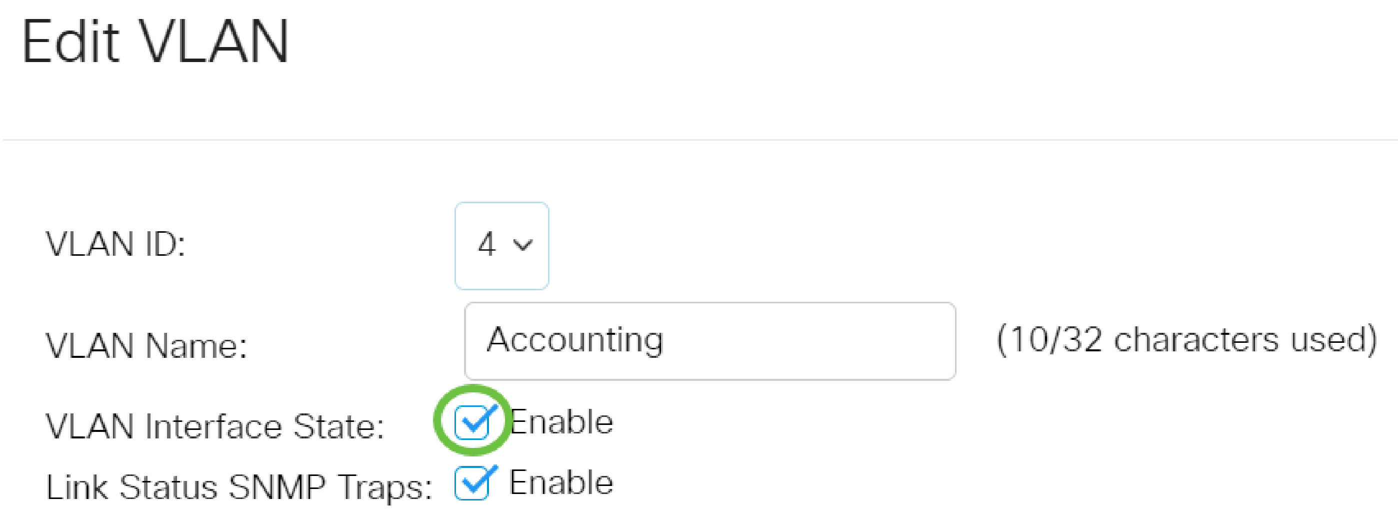
VLAN ID: 4

VLAN Name: Accounting (10/32 characters used)

VLAN Interface State: ☑ Enable

Link Status SNMP Traps: ☑ Enable

Step 6. Check the VLAN Interface State check box to enable the VLAN’s interface state; it is already checked by default. If not, the VLAN will be effectively shut down, and nothing will be able to be transmitted or received through the VLAN.



Edit VLAN

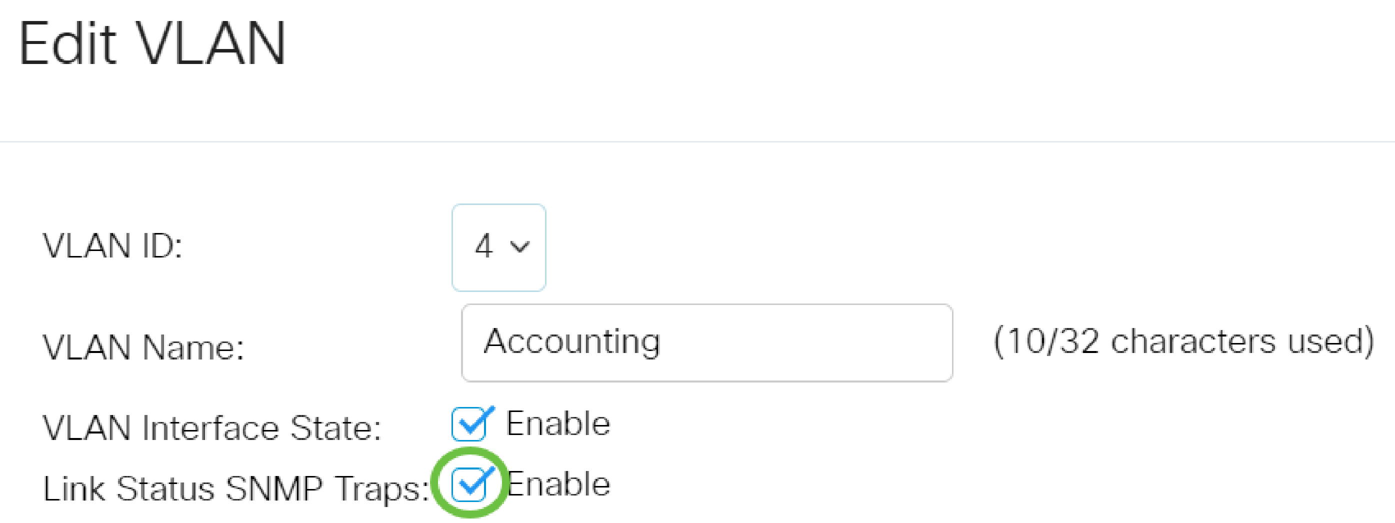
VLAN ID: 4

VLAN Name: Accounting (10/32 characters used)

VLAN Interface State: ☑ Enable

Link Status SNMP Traps: ☑ Enable

Step 7. Check the Enable Link Status SNMP Traps check box to enable the generation of SNMP traps with link status information. This box is checked by default.



Edit VLAN

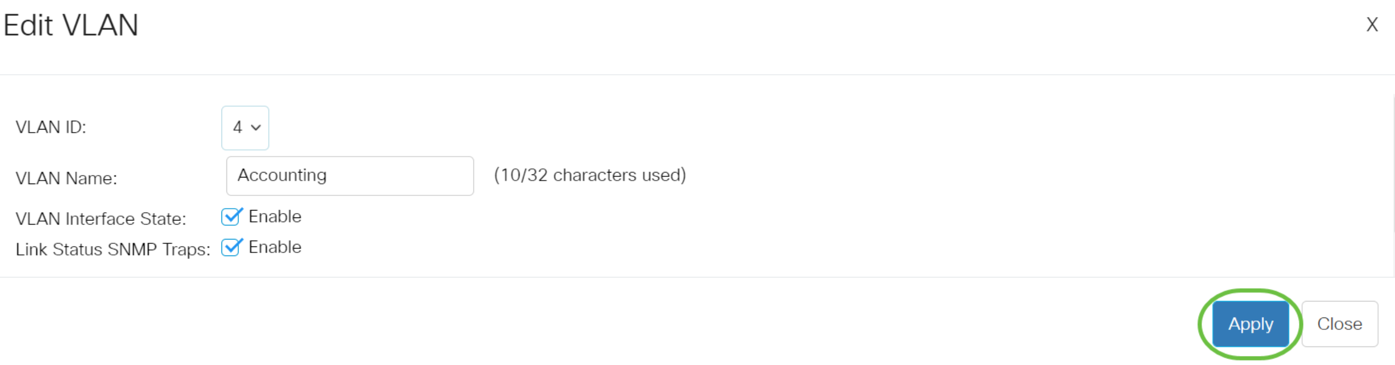
VLAN ID: 4

VLAN Name: Accounting (10/32 characters used)

VLAN Interface State: ☑ Enable

Link Status SNMP Traps: ☑ Enable

Step 8. Click **Apply**.



Edit VLAN x

VLAN ID: 4

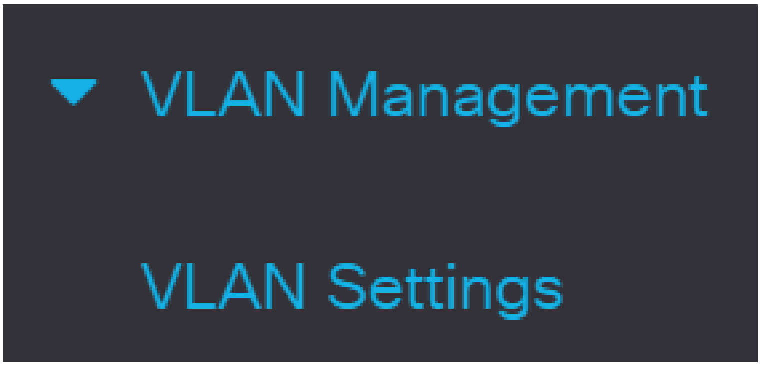
VLAN Name: Accounting (10/32 characters used)

VLAN Interface State: ☑ Enable

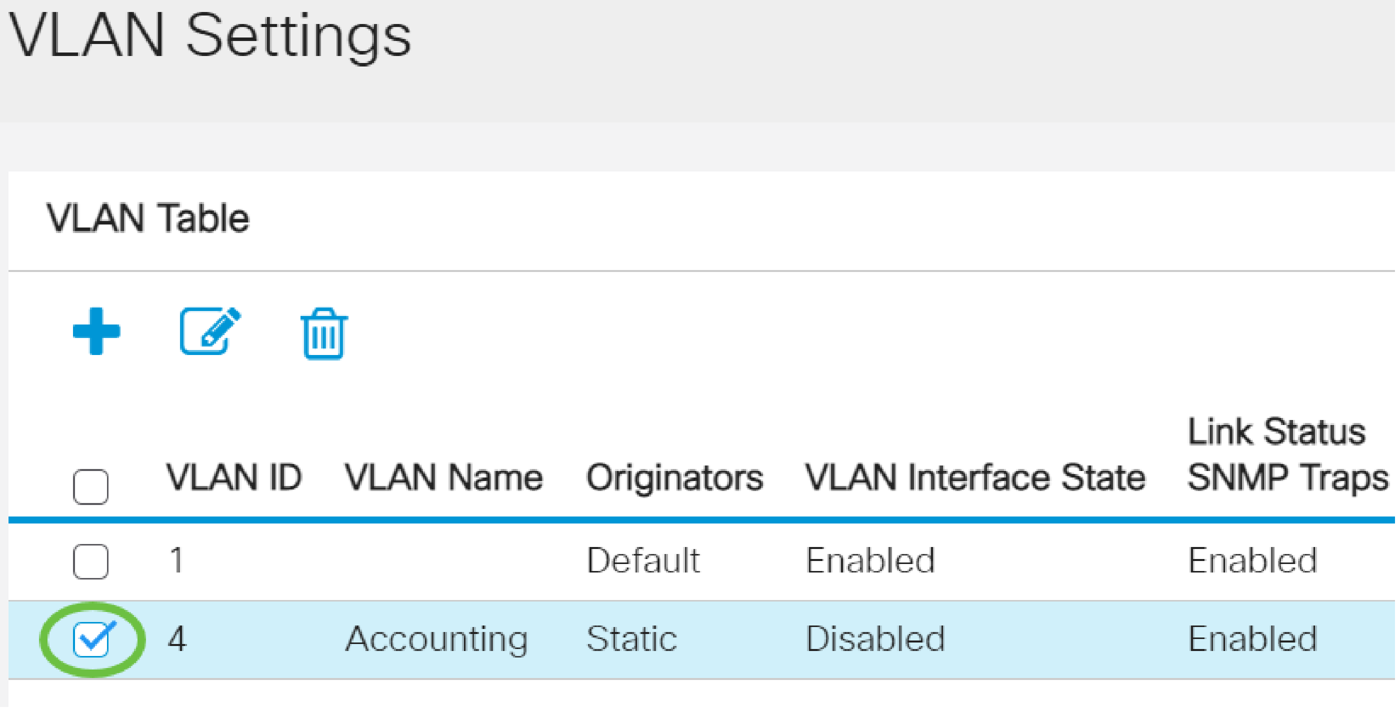
Link Status SNMP Traps: ☑ Enable

Delete a VLAN

Step 1.Log in to the web-based utility and choose **VLAN Management > VLAN Settings**.



Step 2. Check the check box next to the VLAN you want to delete.

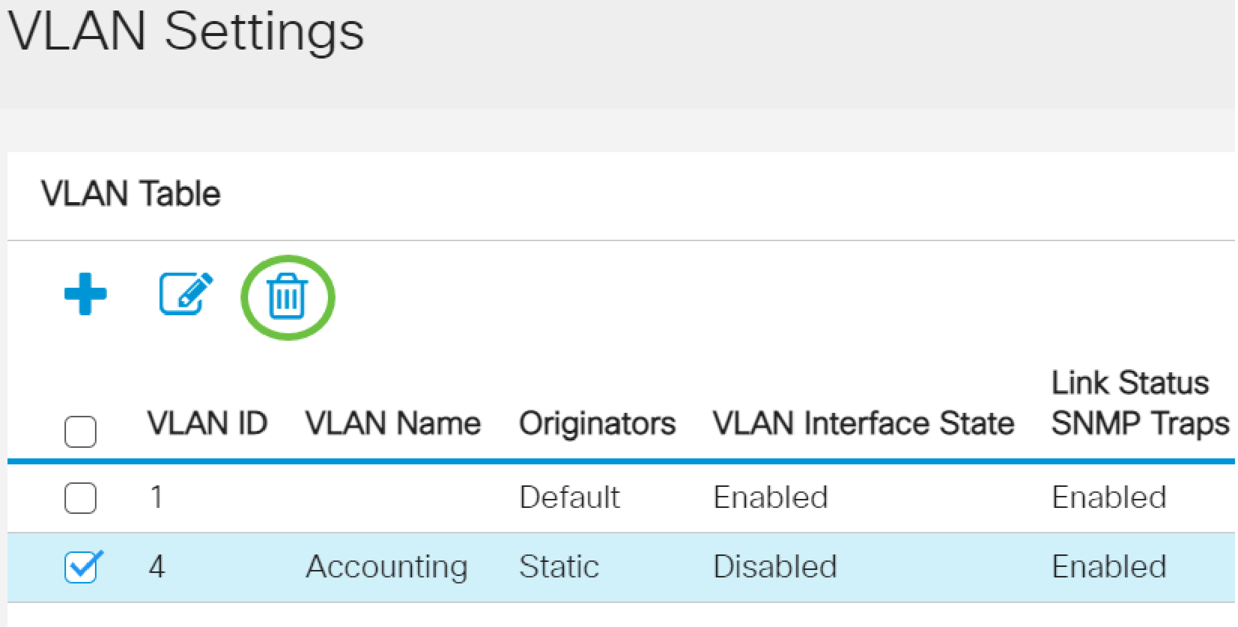


VLAN Settings

VLAN Table

□	VLAN ID	VLAN Name	Originators	VLAN Interface State	Link Status SNMP Traps
□	1		Default	Enabled	Enabled
☑	4	Accounting	Static	Disabled	Enabled

Step 3. Click **Delete** to delete the selected VLAN.



VLAN Settings

VLAN Table

□	VLAN ID	VLAN Name	Originators	VLAN Interface State	Link Status SNMP Traps
□	1		Default	Enabled	Enabled
☑	4	Accounting	Static	Disabled	Enabled

You have now successfully deleted a VLAN on your Cisco Business 250 or 350 series switch.

Looking for more information on VLANs for your Cisco Business Switches? Check out any of the following links for more information.

Port to VLAN Membership **Private VLAN Membership** **Access and Trunk Ports** **Protocol-Based Groups to VLAN** **Port to VLAN Settings** **Subnet-Based VLAN** **Configure Multicast TV Group to VLAN** **Protocol-Based VLAN Groups** **Access Port Multicast TV VLAN Membership** **Customer Port Multicast TV VLAN Membership**

Article Skeleton w/ Content

Objective

The objective of this document is to show you how to configure a basic VLAN via the Command Line Interface (CLI) on Cisco Business 250 or 350 series switches.

Applicable Devices | Software Version

- CBS250 **(DataSheet)** | 3.0.0.69 **(Download latest)**
- CBS350 **(Data Sheet)** | 3.0.0.69 **(Download latest)**
- CBS350-2X **(Data Sheet)** | 3.0.0.69 **(Download latest)**
- CBS350-4X **(Data Sheet)** | 3.0.0.69 **(Download latest)**

Introduction

VLANs allow you to logically segment a LAN into different broadcast domains. In scenarios where sensitive data may be broadcast on a network, VLANs can be created to enhance security by designating a broadcast to a specific VLAN. Only users that belong to a VLAN are able to access and manipulate the data on that VLAN. VLANs can also be used to enhance performance by reducing the need to send broadcasts and multicasts to unnecessary destinations.

Basic VLAN Configuration

Step 1. Login to the switch's Command Line Interface (CLI).

Creating a VLAN

Step 1. Enter the following commands to create a VLAN:

Command	Purpose
`config`	Enter configuration mode.
`vlan database`	Enter VLAN database mode.
`vlan <ID>`	Create a new VLAN with an ID specified.
`end`	Exit from configure mode.

Step 2. (Optional) Enter the following command to display VLAN information:

Command	Purpose
`show vlan`	Display VLAN information.

The VLAN information table will vary depending on the type of switch you are using. The *Ports* field will also vary since different switches have different port types and numbering schemes.

Assigning a Port to a VLAN

Once the VLANs are created, you need to assign the ports to the appropriate VLAN. You can configure ports using the **switchport** command and specify whether the port should be in **access** or **trunk** mode.

The port modes are defined as follows:

- Access - frames received on the interface are assumed to not have a VLAN tag and are assigned to the VLAN indicated by the command. Access ports are used primarily for hosts and can only carry traffic for a single VLAN.
- Trunk - frames received on the interface are assumed to have VLAN tags. Trunk ports are for links between switches or other network devices and are capable of carrying traffic for multiple VLANs.

By default, all interfaces are in trunk mode, which means they can carry traffic for all VLANs.

Step 1. Enter the following commands to configure an access port:

Command	Purpose
`conf t`	Enter configuration mode.
`int <port number>`	Enter interface configuration mode for the specified port number. Gigabit Ethernet, Fast Ethernet and port-channels are valid.
`switchport mode access`	Sets the interface as a nontrunking nontagged single-VLAN Ethernet interface. An access port can carry traffic in one VLAN only.
`switchport access vlan <ID>`	Specifies the VLAN for which this access port will carry traffic.
`no shut`	Turn on (enable) the port.
`end`	Exit from configure mode.

Step 2. (Optional) Enter the **show vlan** command to see your assigned port.

```
CBS350#show vlan
```

Step 3. Enter the following commands to configure a trunk port and specify that only certain VLANs are allowed on the specified trunk:

Command	Purpose
`conf t`	Enter configuration mode.
`int <port number>`	Enter interface configuration mode for the specified port number. Gigabit Ethernet, Fast Ethernet and port-channels are valid.
`switchport mode trunk`	Make the specified port number aware of all VLANs.
`switchport trunk allowed vlan add <ID>`	Makes the port a member in the specified VLAN ID and gives it an Egress Rule: Tagged. This means packets are tagged with the VLAN ID as they leave this port on the device.
`no shut`	Turn on (enable) the port.
`end`	Exit from configure mode.

In trunk mode, all VLANs are allowed by default. Using the
add command lets you configure the VLANs allowed on the trunk.

Step 4. (Optional) Enter the **show vlan** command to see your changes.

```
CBS350#show vlan
```

Step 5. (Optional) Enter the following command to display information about a port:

Command	Purpose
`show interfaces switchport <port number>`	Display information such as VLAN membership, the Egress rule, and forbidden VLANs for the specified port.

For more information, check out the links below.

- **Configure Port Virtual Local Area Network (VLAN) Membership of an Interface on a Cisco Business 250 or 350 Series Switch**
- **Configure Private Virtual Local Area Network (VLAN) Settings on a Cisco Business 250 or 350 Series Switch**
- **Configure Port to VLAN Interface Settings on a Cisco Business 250 or 350 Series Switch through the CLI**
- **Configure Private VLAN Membership Settings on a Cisco Business 250 or 350 Series Switch through the CLI**

Looking for more information on VLANs for your Cisco Business Switches? Check out any of the following links for more information.

Port to VLAN Membership **Private VLAN Membership** **Access and Trunk Ports** **Protocol-Based Groups to VLAN** **Port to VLAN Settings** **Subnet-Based VLAN** **Configure Multicast TV Group to VLAN** **Protocol-Based VLAN Groups** **Access Port Multicast TV VLAN Membership** **Customer Port Multicast TV VLAN Membership**