Private VLAN Membership on a Cisco Business 350 Switch

Objective

This article provides instructions on how to configure private VLAN settings on a Cisco Business 350 series switch.

Applicable Devices | Software Version

- 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

A Virtual Local Area Network (VLAN) allows you to logically segment a Local Area Network (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.

A Private VLAN provides layer-2 isolation between ports. This means that at the level of bridging traffic, as opposed to IP routing, ports that share the same broadcast domain cannot communicate with each other. The ports in a private VLAN can be located anywhere in the layer 2 network, which means they do not have to be on the same switch. The private VLAN is designed to receive untagged or priority-tagged traffic and transmit untagged traffic.

The following types of ports can be members in a private VLAN:

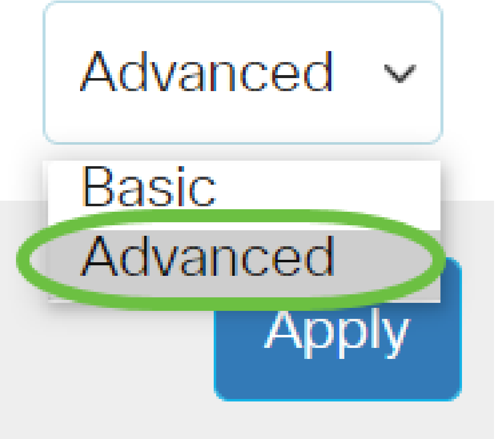
- Promiscuous - A promiscuous port can communicate with all ports of the same private VLAN. These ports connect servers and routers.
- Community (host) - Community ports can define a group of ports that are member in the same Layer 2 domain. They are isolated at Layer 2 from other communities and from isolated ports. These ports connect host ports.
- Isolated (host) - An isolated port has complete Layer 2 isolation from the other isolated and community ports within the same private VLAN. These ports connect host ports.

Host traffic is sent on isolated and community VLANs, while server and router traffic is sent on the primary VLAN.

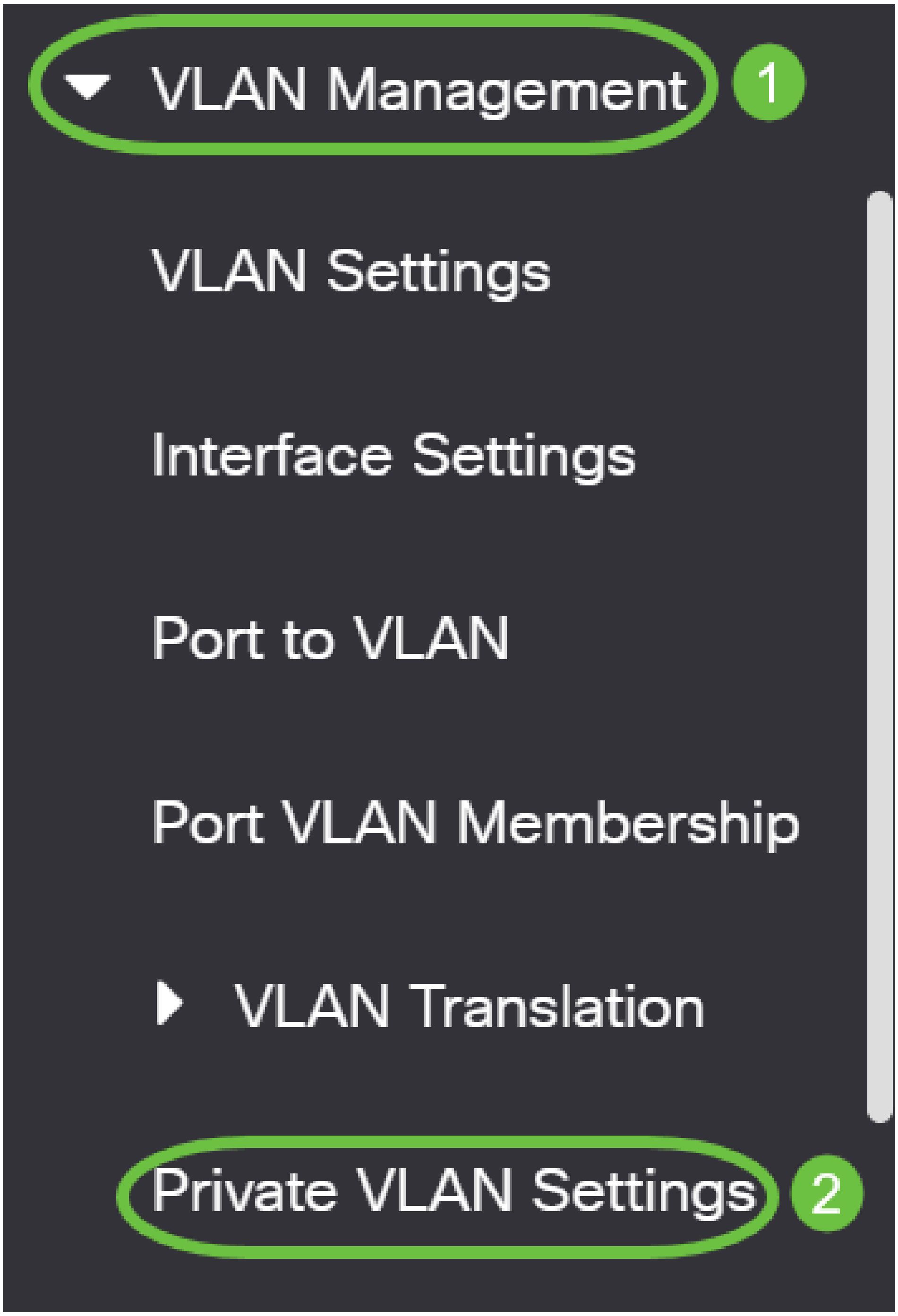
Configure Private VLAN Settings on a Switch

Important: Before proceeding with the steps below, make sure VLANs have been configured on the switch. To know how to configure VLAN settings on your switch, click here for instructions.

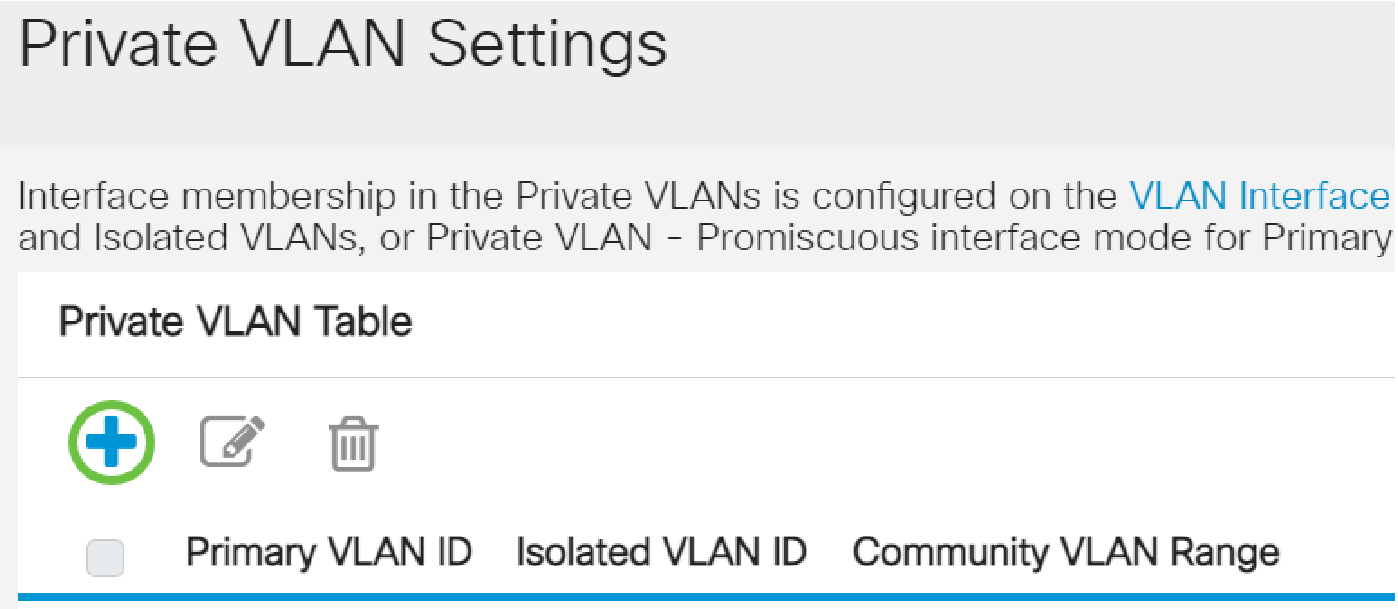
Step 1. Log in to the web-based utility and choose **Advanced** from the Display Mode drop-down list.



Step 2. Choose **VLAN Management >Private VLAN Settings**.



Step 3. Click the **Add** button.



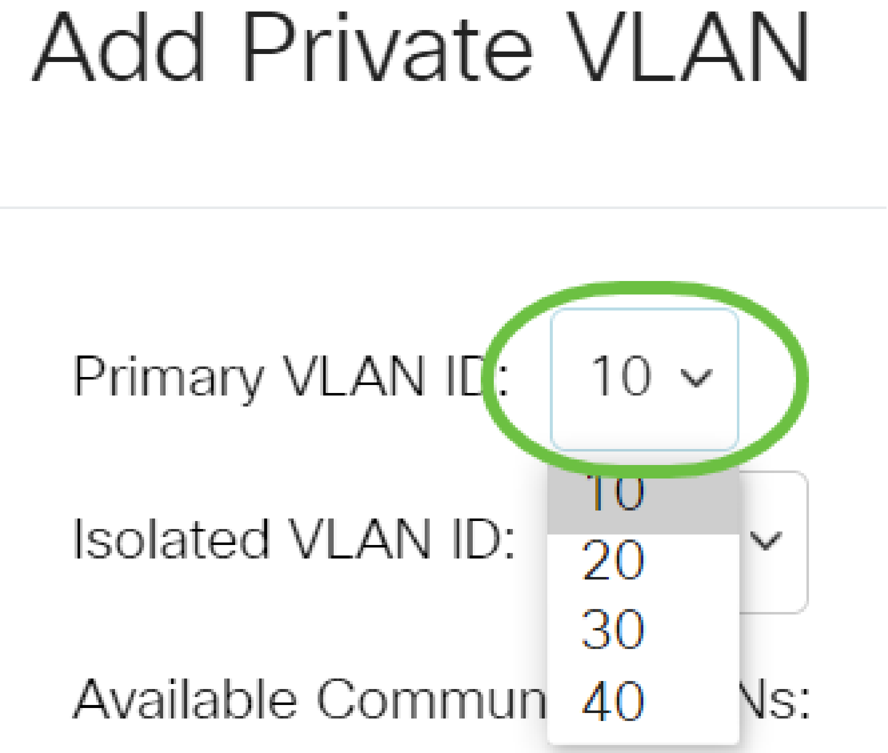
Private VLAN Settings

Interface membership in the Private VLANs is configured on the VLAN Interface
and Isolated VLANs, or Private VLAN - Promiscuous interface mode for Primary

Private VLAN Table

□	Primary VLAN ID	Isolated VLAN ID	Community VLAN Range

Step 4. In the Primary VLAN ID drop-down list, choose a VLAN to be defined as the primary VLAN in the private VLAN. The primary VLAN is used to allow Layer 2 connectivity from promiscuous ports to isolated ports and to community ports.



Add Private VLAN

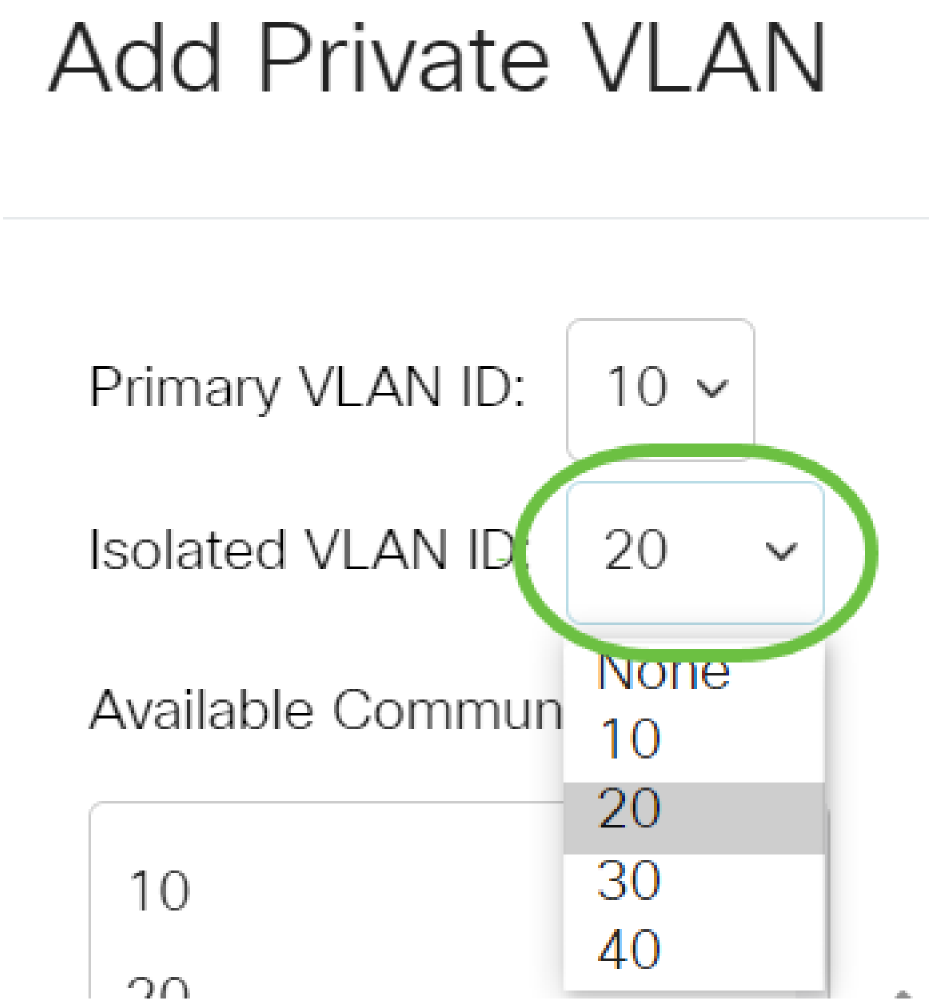
Primary VLAN ID: 10

Isolated VLAN ID:

Available Commun Ns:

Note: In this example, VLAN ID 10 is chosen.

Step 5. Choose a VLAN ID from the Isolated VLAN ID drop-down list. An isolated VLAN is used to allow isolated ports to send traffic to the primary VLAN.



Add Private VLAN

Primary VLAN ID: 10

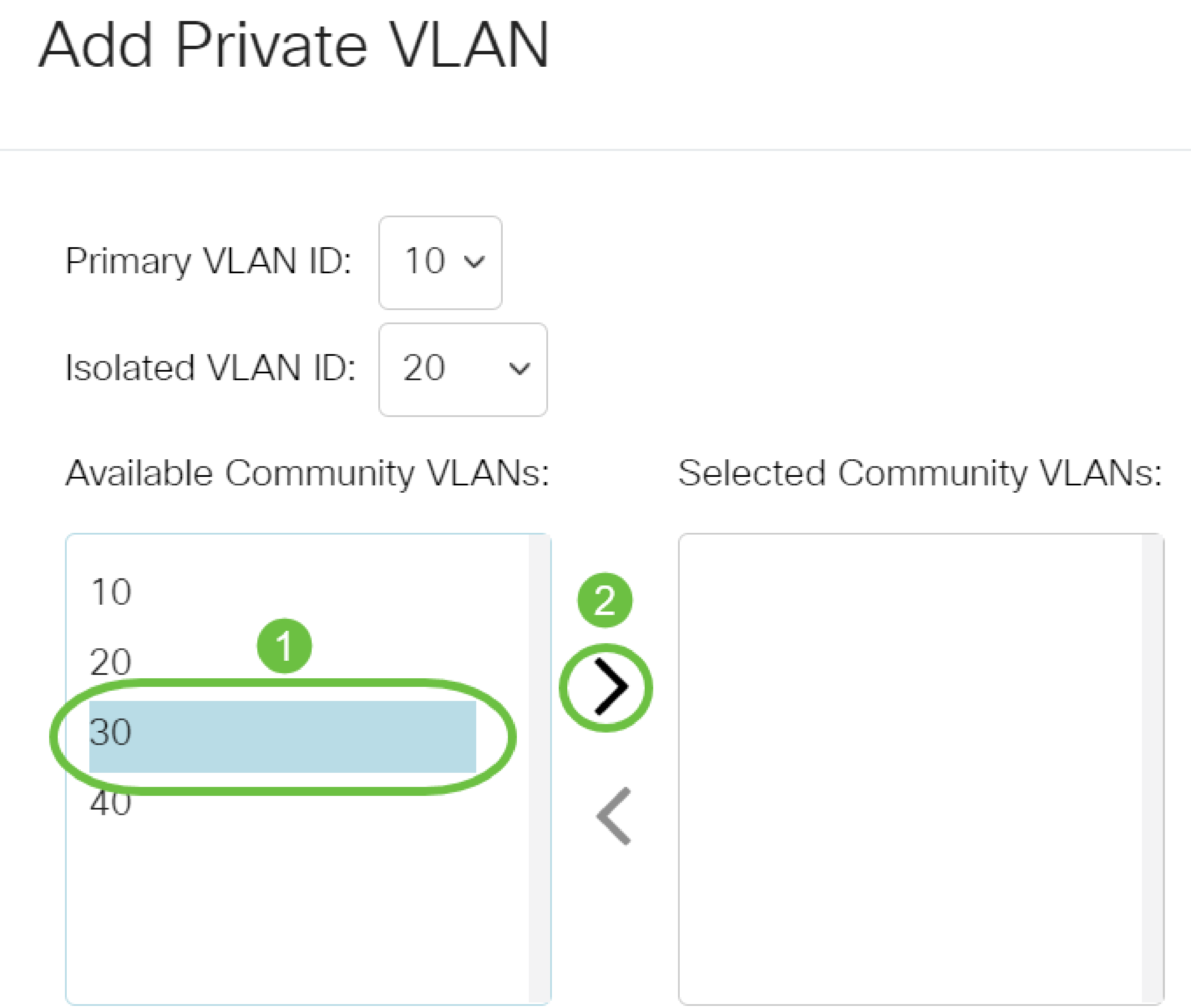
Isolated VLAN ID: 20

Available Commun

Note: In this example, VLAN ID 20 is chosen.

Step 6. Choose a VLAN ID from the Available Community VLANs area then click the **>** button to move the VLANs that you want to be community VLANs to the Selected Community VLANs list.

Note: To create a sub-group of ports (community) within a VLAN, the ports must be added a community VLAN. The community VLAN is used to enable Layer 2 connectivity from community ports to promiscuous ports and to community ports of the same community. There can be a single community VLAN for each community and multiple community VLANs can coexist in the system for the same private VLAN.



Add Private VLAN

Primary VLAN ID: 10

Isolated VLAN ID: 20

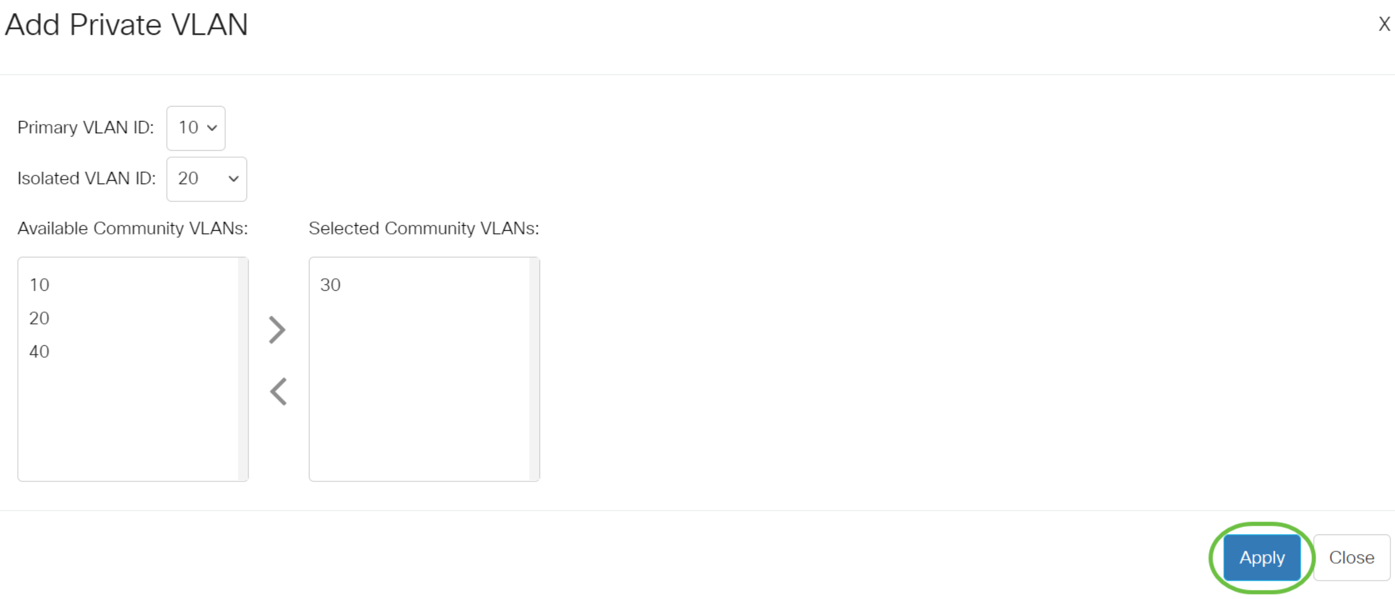
Available Community VLANs:

10
20
30
40

Selected Community VLANs:

Note: In this example, VLAN ID 30 is chosen.

Step 7. Click **Apply** then click **Close**.



Add Private VLAN

Primary VLAN ID: 10

Isolated VLAN ID: 20

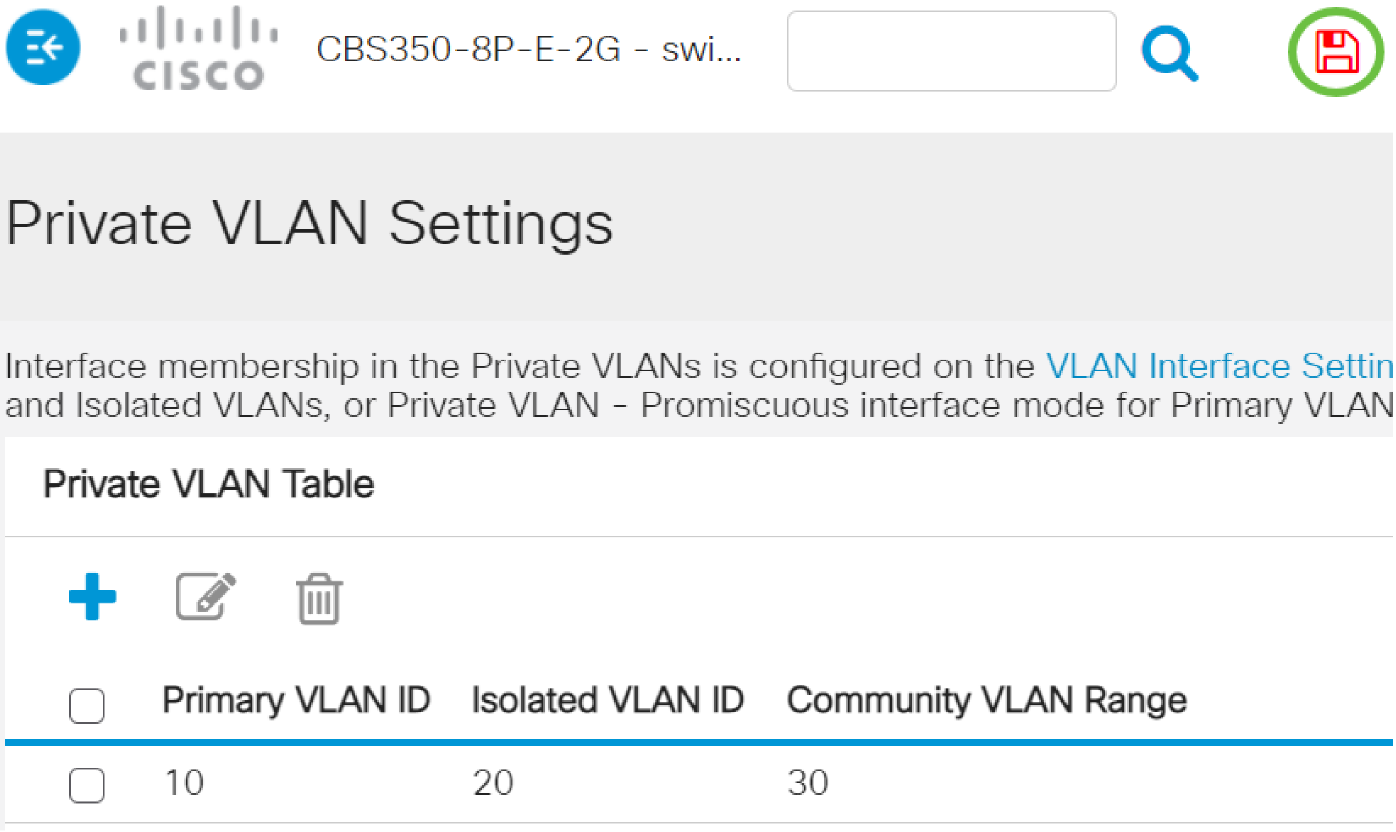
Available Community VLANs:

10
20
40

Selected Community VLANs:

30

Step 8. (Optional) Click **Save** to save settings to the startup configuration file.



CBS350-8P-E-2G - swi...

Private VLAN Settings

Interface membership in the Private VLANs is configured on the VLAN Interface Settin
and Isolated VLANs, or Private VLAN - Promiscuous interface mode for Primary VLAN

Private VLAN Table

□	Primary VLAN ID	Isolated VLAN ID	Community VLAN Range
□	10	20	30

You have now configured the private VLAN settings on your Cisco Business 350 series switch.

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

Create VLANs **Port to 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

This article provides instructions on how to configure private VLAN settings on a Cisco Business 350 series switch.

A Private VLAN provides layer-2 isolation between ports. This means that at the level of bridging traffic, as opposed to IP routing, ports that share the same broadcast domain cannot communicate with each other. The ports in a private VLAN can be located anywhere in the layer 2 network, which means they do not have to be on the same switch. The private VLAN is designed to receive untagged or priority-tagged traffic and transmit untagged traffic.

Applicable Devices | Software Version

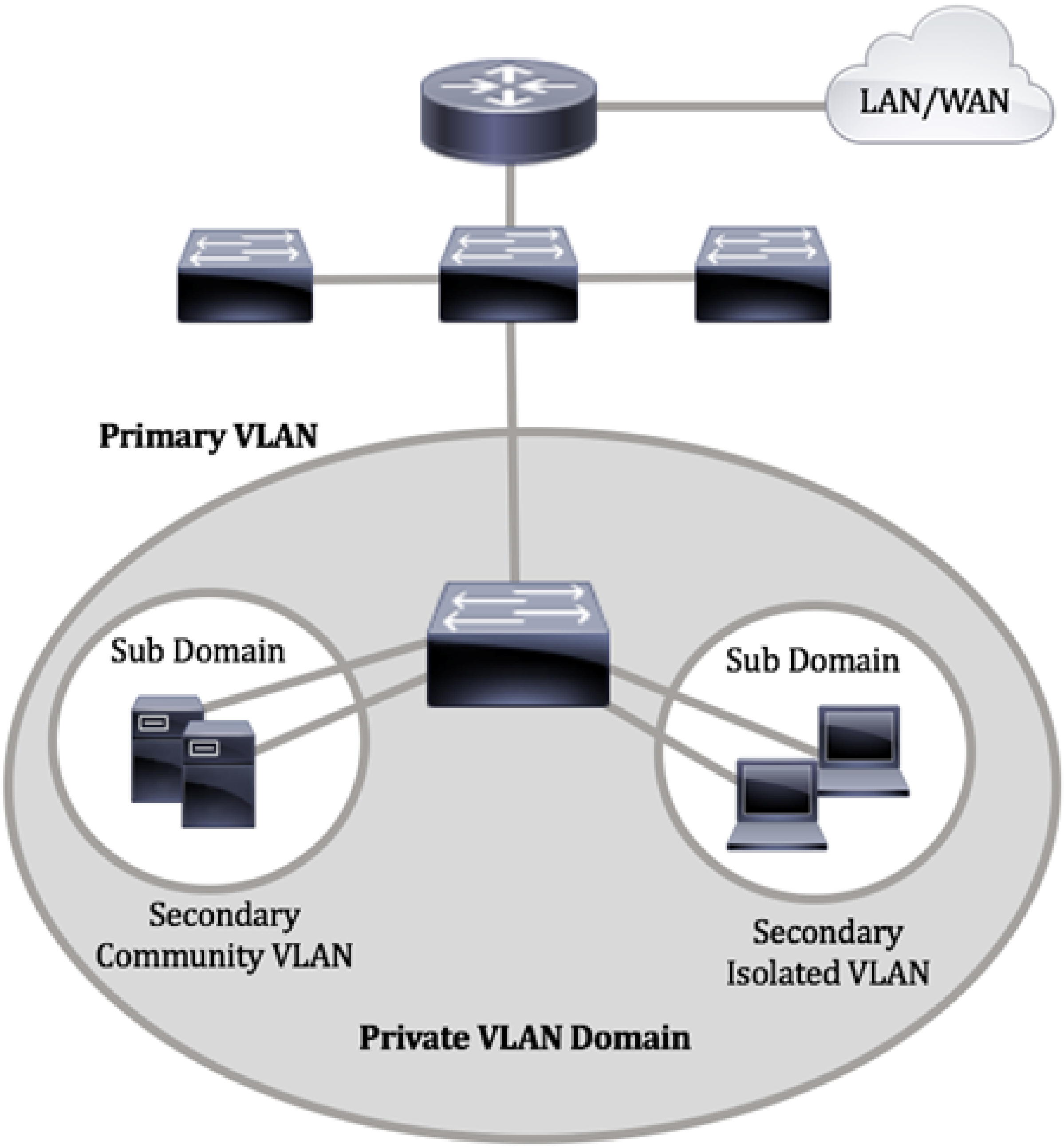
- CBS350 **(Data Sheet)** | 3.0.0.69 **(Download latest)**
- CBS350-2X **(Data Sheet)** | 3.0.0.69 **(Download latest)**
- CBS350-4X **(Data Sheet)** | 3.0.0.69 **(Download latest)**

Introduction

A Virtual Local Area Network (VLAN) allows you to logically segment a Local Area Network (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.

Note: To learn how to configure the VLAN settings on your switch through the web-based utility, click **here**. For CLI-based instructions, click **here**.

A Private VLAN domain consists of one or more pairs of VLANs. The primary VLAN makes up the domain; and each VLAN pair makes up a subdomain. The VLANs in a pair are called the primary VLAN and the secondary VLAN. All VLAN pairs within a private VLAN have the same primary VLAN. The secondary VLAN ID is what differentiates one subdomain from another.



A private VLAN domain has only one primary VLAN. Each port in a private VLAN domain is a member of the primary VLAN; the primary VLAN is the entire private VLAN domain.

Secondary VLANs provide isolation between ports within the same private VLAN domain. The following two types are secondary VLANs within a primary VLAN:

- Isolated VLANs - Ports within an isolated VLAN cannot communicate directly with each other at the Layer 2 level.
- Community VLANs - Ports within a community VLAN can communicate with each other but cannot communicate with ports in other community VLANs or in any isolated VLANs at the Layer 2 level.

Within a private VLAN domain, there are three separate port designations. Each port designation has its own unique set of rules which regulate the ability of one endpoint to communicate with other connected endpoints within the same private VLAN domain. The following are the three port designations:

- Promiscuous - A promiscuous port can communicate with all ports of the same private VLAN. These ports connect servers and routers.
- Community (host) - Community ports can define a group of ports that are member in the same Layer 2 domain. They are isolated at Layer 2 from other communities and from isolated ports. These ports connect host ports.
- Isolated (host) - An isolated port has complete Layer 2 isolation from the other isolated and community ports within the same private VLAN. These ports connect host ports.

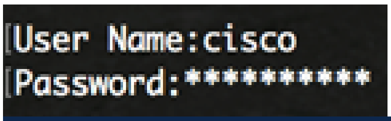
Host traffic is sent on isolated and community VLANs, while server and router traffic is sent on the primary VLAN.

To configure the private VLAN using the web-based utility of the switch, click here.

Configure Private VLAN Settings on the Switch through the CLI

Create a Private Primary VLAN

Step 1. Log in to the switch console. The default username and password is cisco/cisco. If you have configured a new username or password, enter the credentials instead.



```
[User Name:cisco
[Password:**********
```

The commands may vary depending on the exact model of your switch.

Step 2. From the Privileged EXEC mode of the switch, enter the Global Configuration mode by entering the following:

```
CBS350#configure
```

Step 3. In the Global Configuration mode, enter the Interface Configuration context by entering the following:

```
CBS350(config)#interface [vlan-id]
```

- vlan-id - Specifies the VLAN ID to be configured.

Step 4. In the Interface Configuration context, configure the VLAN interface as the primary private VLAN by entering the following:

```
CBS350(config-if)#private-vlan primary
```

By default, there are no private VLANs configured on the switch.

Important: Make sure to remember the following guidelines in configuring a private VLAN:

- The VLAN type cannot be changed if there is a private VLAN port that is a member in the VLAN.
- The VLAN type cannot be changed if it is associated with other private VLANs.
- The VLAN type is not kept as a property of the VLAN when the VLAN is deleted.

Step 5. (Optional) To return the VLAN to its normal VLAN configuration, enter the following:

```
CBS350(config-if)#no private-vlan
```

Step 6. (Optional) To go back to the Privileged EXEC mode of the switch, enter the following:

```
CBS350(config-if)#end
```

Step 7. (Optional) In the Privileged EXEC mode of the switch, save the configured settings to the startup configuration file, by entering the following:

```
CBS350#copy running-config startup-config
```

Step 8. (Optional) Press **Y** for Yes or **N** for No on your keyboard once the Overwrite file [startup-config]… prompt appears.

You have now successfully created the primary VLAN on your switch through the CLI.

Create a Secondary VLAN

Step 1. In the Privileged EXEC mode of the switch, enter the Global Configuration mode by entering the following:

```
CBS350#configure
```

Step 2. In the Global Configuration mode, enter the Interface Configuration context by entering the following:

```
CBS350(config)#interface [vlan-id]
```

Step 3. In the Interface Configuration context, configure the VLAN interface as the secondary private VLAN by entering the following:

```
CBS350(config-if)#private-vlan [community | isolated]
```

The options are:

- community - Designate the VLAN as a community VLAN.
- isolated - Designate the VLAN as an isolated VLAN.

Step 4. (Optional) Repeat steps 2 and 3 to configure additional secondary VLAN for your private VLAN.

Step 5. (Optional) To return the VLAN to its normal VLAN configuration, enter the following:

```
CBS350(config-if)#no private-vlan
```

Step 6. (Optional) To go back to the Privileged EXEC mode of the switch, enter the following:

```
CBS350(config-if)#end
```

You have now successfully created secondary VLANs on your switch through the CLI.

Associate the Secondary VLAN to the Primary Private VLAN

Step 1. In the Privileged EXEC mode of the switch, enter the Global Configuration mode by entering the following:

```
CBS350#configure
```

Step 2. Enter the VLAN Interface Configuration context of the primary VLAN by entering the following:

```
CBS350(config)#vlan [primary-vlan-id]
```

Step 3. To configure the association between the primary VLAN and secondary VLANs, enter the following:

```
CBS350(config-if)#private-vlan association [add |
remove]secondary-vlan-list
```

The options are:

- **add** secondary-vlan-list - List of VLAN IDs of type secondary to add to a primary VLAN. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs. This is the default action.
- **remove** secondary-vlan-list - List of VLAN IDs of type secondary to remove association from a primary VLAN. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.

Step 4. To go back to the Privileged EXEC mode of the switch, enter the following:

```
CBS350(config-if)#end
```

You have now successfully associated the secondary VLANs to the primary private VLAN on your switch through the CLI.

Configure Ports to the Primary and Secondary Private VLANs

Step 1. In the Privileged EXEC mode of the switch, enter the Global Configuration mode by entering the following:

```
CBS350#configure
```

Step 2. In the Global Configuration mode, enter the Interface Configuration context by entering the following:

```
CBS350(config)#interface [interface-id | range vlan vlan-range]
```

The options are:

- interface-id - Specifies an interface ID to be configured.
- range vlan vlan-range - Specifies a list of VLANs. Separate nonconsecutive VLANs with a comma and no spaces. Use a hyphen to designate a range of VLANs.

Step 3. In the Interface Configuration context, use the **switchport mode** command to configure the VLAN membership mode.

```
CBS350(config-if-range)#switchport mode private-vlan [promiscuous | host]
```

- promiscuous - Specifies a private VLAN promiscuous port. If this option is used, skip to **Step 5**.
- host - Specifies a private VLAN host port. If this option is used, skip to **Step 6**.

Step 4. (Optional) To return the port or range of ports to the default configuration, enter the following:

```
CBS350(config-if-range)#no switchport mode
```

Step 5. To configure the association of a promiscuous port with primary and secondary VLANs of the private VLAN, enter the following:

```
CBS350(config-if)#switchport private-vlan mapping [primary-vlan-id] add [secondary-vlan-id]
```

The options are:

- primary-vlan-id - Specifies the VLAN ID of the primary VLAN.
- secondary-vlan-id - Specifies the VLAN ID of the secondary VLAN.

Step 6. To configure the association of a host port with primary and secondary VLANs of the private VLAN, enter the following:

```
CBS350(config-if)#switchport private-vlan host-association[primary-vlan-id][secondary-vlan-id]
```

The options are:

- primary-vlan-id - Specifies the VLAN ID of the primary VLAN.
- secondary-vlan-id - Specifies the VLAN ID of the secondary VLAN.

Step 7. To exit the Interface Configuration context, enter the following:

```
CBS350(config-if-range)#exit
```

Step 8. (Optional) Repeat steps 2 to 7 to configure more promiscuous and host ports and assign to the corresponding primary and secondary private VLANs.

Step 9. Enter the **end** command to go back to the Privileged EXEC mode:

```
CBS350(config-if)#end
```

Step 10. (Optional) To verify the configured private VLANs on your switch, enter the following:

```
CBS350#show vlan private-vlan tag[vlan-id]
```

Step 11. (Optional) In the Privileged EXEC mode of the switch, save the configured settings to the startup configuration file, by entering the following:

```
CBS350#copy running-config startup-config
```

Step 12. (Optional) Press **Y** for Yes or **N** for No on your keyboard once the Overwrite file [startup-config]… prompt appears.

You have now successfully configured the association of host and promiscuous ports with primary and secondary private VLANs on your 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.

Create VLANs **Port to 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**