Configure VLAN Mapping on a Switch through the CLI

Objective

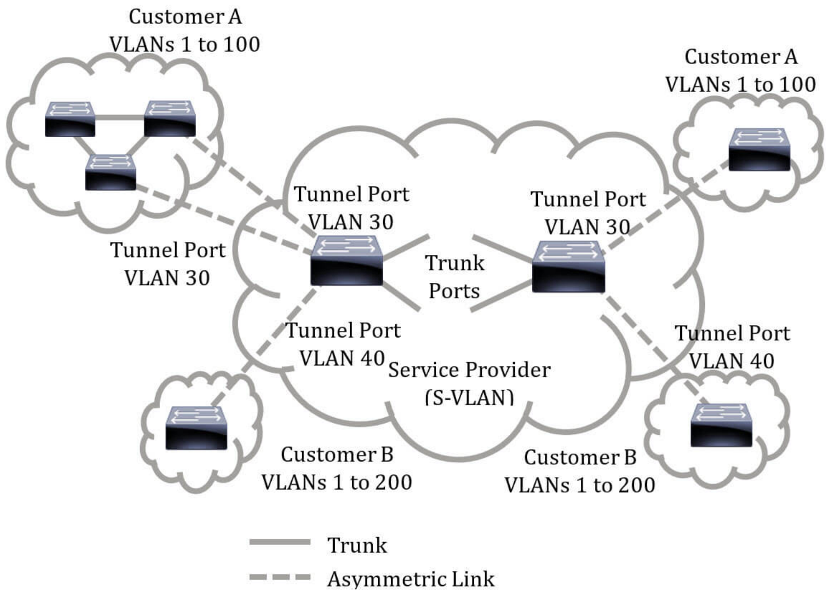
This article provides instructions on how to configure the Virtual Local Area Network (VLAN) mapping settings on your switch through the Command Line Interface (CLI).

Introduction

To establish Service Provider Virtual Local Area Networks (S-VLANs), you can configure VLAN mapping or VLAN ID translation on trunk ports that are connected to a customer network. This will map customer VLANs to service provider. Packets entering the port are mapped to S-VLAN based on the port number and the original customer VLAN-ID (C-VLAN) of the packet.

In a typical metro deployment, VLAN mapping takes place on user network interfaces (UNIs) or enhanced network interfaces (ENIs) that face the customer network. However, you are not prevented from configuring VLAN mapping on network node interfaces (NNIs).

The image below displays an example of a network where a customer uses the same VLANs in multiple sites on different sides of a service provider network.



You can map the C-VLAN IDs to S-VLAN IDs for packet travel across the service provider backbone. The C-VLAN IDs are retrieved at the other side of the service provider backbone for use in the other customer site. You can configure the same set of VLAN mappings at a customer-connected port on each side of the service provider network.

VLAN Tunneling

VLAN tunneling is an enhancement of the QinQ or Nested VLAN or the Customer mode VLAN feature. It enables service providers to use a single VLAN to support customers who have multiple VLANs, while preserving customer VLAN IDs and keeping traffic in different customer VLANs segregated. This feature is known as double tagging or QinQ because in addition to the regular 802.1Q tag, which is also known as the C-VLAN, the switch adds a second ID tag known as the S-VLAN, to forward traffic over the network. On an edge interface, which is an interface where a customer network is connected to the provider edge switch, C-VLANs are mapped to S-VLANs and the original C-VLAN tags are kept as part of the payload. Untagged frames are dropped.

When a frame is sent on a non-edge tagged interface, it is encapsulated with another layer of S-VLAN tag to which the original C-VLAN-ID is mapped. Therefore, packets transmitted on non-edge interfaces frames are double-tagged, with an outer S-VLAN tag and inner C-VLAN tag. The S-VLAN tag is preserved while traffic is forwarded through the network infrastructure of the service provider. On an egress device, the S-VLAN tag is stripped when a frame is sent out on an edge interface. Untagged frames are dropped.

The VLAN tunneling feature uses a different set of commands than the original QinQ or Nested VLAN implementation, and adds the following functionality in addition to the original implementation:

- Provides multiple mappings of different C-VLANs to separate S-VLANs per edge interface.
- Allows the configuration of a drop action for certain C-VLANs received on edge interfaces.
- Allows the configuration of the action for C-VLANs which are not specifically mapped to an S-VLAN (drop or map to certain S-VLANs).
- Allows the global configuration and per NNI (backbone ports) which is the Ethertype of the S-VLAN tag. In the previous QinQ implementation, only the Ethertype of 0x8100 was supported for an S-VLAN tag.

You must create and specify the S-VLAN on the device before configuring it on an interface as an S-VLAN. If this VLAN does not exist, the command fails.

The IPv4 or IPv6 forwarding and VLAN tunneling are mutually exclusive. Meaning that if either IPv4 or IPv6 forwarding are enabled, an interface cannot be set to VLAN tunneling mode. And if any interface is set to VLAN tunneling mode, both IPv4 and IPv6 forwarding cannot be enabled on that device.

The following features are also mutually exclusive with the VLAN tunneling feature:

- Auto Voice VLAN
- Auto Smartport
- Voice VLAN

The IPv4 and IPv6 interfaces cannot be defined on VLANs containing edge interfaces.

The following Layer 2 features are not supported on VLANs containing edge interfaces:

- Internet Group Management Protocol (IGMP) or Multicast Listener Discovery (MLD) snooping
- Dynamic Host Configuration Protocol (DHCP) Snooping
- IPv6 First Hop Security

The following features are not supported on edge interfaces or UNI:

- Remote Authentication Dial-In User Service (RADIUS) VLAN assignment
- 802.1x VLAN
- Switch Port Analyzer (SPAN) or Remote SPAN (RSPAN) - As a destination port with the network keyword or as a reflector port destination port with the network keyword or reflector

port.

The original QinQ implementation (customer mode-related commands) continues to exist alongside the new implementation of VLAN tunneling. The customer port mode is a particular case of VLAN-mapping tunnel port mode, and does not require allocation of Ternary Content Addressable Memory (TCAM) resources.

VLAN One-to-One Mapping

In addition to VLAN tunneling, the switch supports VLAN One-to-One Mapping. In VLAN One-to-One Mapping, on an edge interface, C-VLANs are mapped to S-VLANs and the original C-VLAN tags are replaced by the specified S-VLAN. Untagged frames are dropped.

When a frame is sent on non-edge tagged interface, it is sent with a single VLAN tag, namely that of the specified S-VLAN. The S-VLAN tag is preserved while traffic is forwarded through the infrastructure network of the service provider. On the egress device, the S-VLAN tag is replaced with the C-VLAN tag when a frame is sent to an edge interface.

In the VLAN mapping one-to-one mode, an interface belongs to all S-VLANs for which mapping on this interface is defined as an egress-tagged interface. The interface port VLAN ID (PVID) is set to 4095.

Prerequisites in configuring VLAN Mapping on your switch:

1. Create the VLANs. To learn how to configure the VLAN settings on your switch through the CLI, click here.
2. Disable IP routing on the switch. To learn how to configure IP routing settings on your switch through the CLI, click here.
3. Configure TCAM allocations on your switch. To learn how to configure router TCAM resources allocation for VLAN tunneling and mapping purposes through the CLI, click here.

   Note: Applying VLAN tunneling on an interface requires the use of router TCAM rules. There should be four TCAM entries per mapping. If there is not a sufficient number of router TCAM resources, the command will fail.

1. Disable Spanning Tree Protocol (STP) on the interfaces that you want to configure. For instructions on how to configure the STP interface settings on your switch through the CLI, click here.
2. Disable Generic Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP) on the interface. To learn how to configure the GVRP settings on your switch through the CLI, click here.

Applicable Devices

- Sx350 Series
- SG350X Series
- Sx550X Series

Software Version

- 2.3.0.130

Configure VLAN Mapping

Configuring VLAN Tunnel Mapping on the switch performs the following actions:

- Creates an Access Control List (ACL) for mapping VLANs from VLAN List to Outer VLAN ID.
- Adds to the ACL one rule for each VLAN from the VLAN List.
- Reserves the place into Tunnel Termination and Interface (TTI) for this ACL. If there is not enough free place into TTI, the command fails.

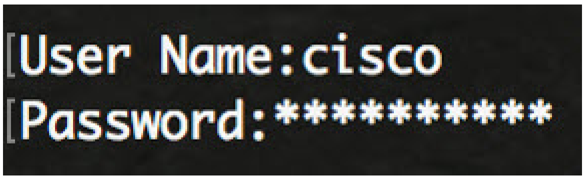
Note: The ACL can be bound on the interface later through the configuration of One-to-One VLAN Mapping.

- Adds the edge interface to the VLAN specified in the Outer VLAN ID.
- The ACL contains V+1 rules, where V is the number of specified C-VLANs.

Follow these steps to configure tunnel mapping on a specific interface or interfaces of your switch:

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.

Note: To learn how to access an SMB switch CLI through SSH or Telnet, click here.



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

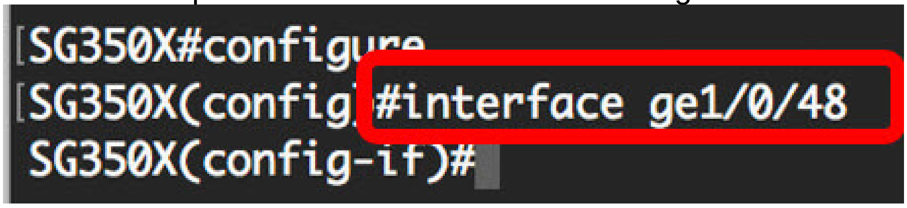
Note: The commands may vary depending on the exact model of your switch. In this example, the SG350X switch is accessed through Telnet.

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

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

The options are:

- interface-id - Specifies an interface ID to be configured.



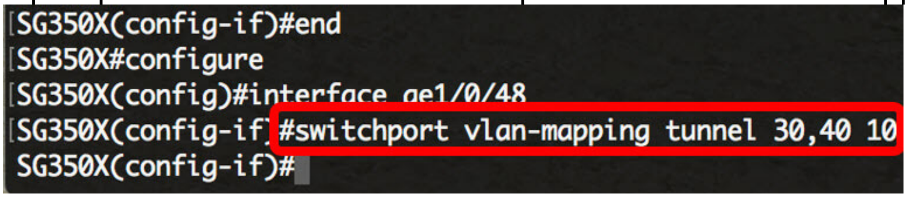
```
SG350X#configure
SG350X(config)#interface ge1/0/48
SG350X(config-if)#
```

Note: In this example, the interface used is ge1/0/48 is being configured.

Step 4. To configure selective tunneling on an edge interface, enter the following:

The parameters are:

- vlan-list - Specifies the C-VLANs for selective tunneling. The VLAN IDs in the list are separated by a comma or a series of VLAN IDs separated by a hyphen (such as 1,2,3-5). The range is from one to 4094.
- default - Specifies the list of the C-VLANs other than those not specified. If a default action is not configured, the input frames with unspecified C-VLANs are dropped.
- outer-vlan-id - Specifies the added an outer S-VLAN tag. The range of the S-VLAN tag is one to 4094.
- drop - Specifies that frames with the specified C-VLANs are dropped.

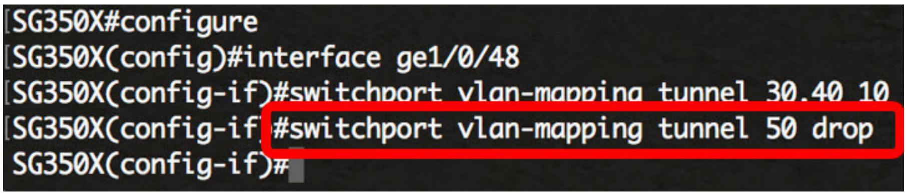


```
[SG350X(config-if)#end
[SG350X#configure
[SG350X(config)#interface ge1/0/48
[SG350X(config-if)#switchport vlan-mapping tunnel 30,40 10
 SG350X(config-if)#
```

Note: This example shows how to configure selective tunneling on the interface ge1/0/48 so that the traffic with a C-VLAN ID of 30 and 40 would be tunneled with S-VLAN ID of 10.

Quick Tip: You can define a few switchport configurations on the same interface, only if the VLAN List arguments do not contain common VLAN IDs.

Step 5. (Optional) Repeat Step 4 to configure more Tunnel Mapping settings on the port or Steps 3 and 4 to configure other ports.

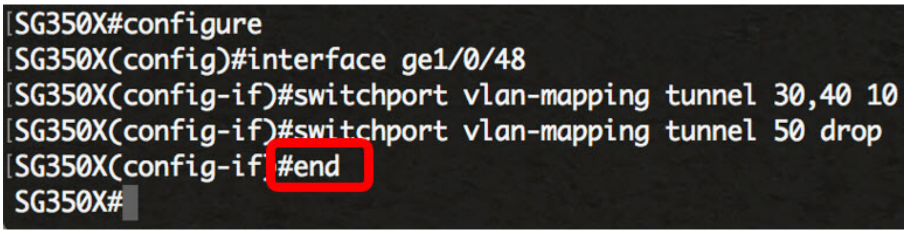


```
[SG350X#configure
[SG350X(config)#interface ge1/0/48
[SG350X(config-if)#switchport vlan-mapping tunnel 30,40 10
[SG350X(config-if)#switchport vlan-mapping tunnel 50 drop
 SG350X(config-if)#
```

Note: In this example, the traffic entering interface ge1/0/48 from VLAN 50 will be dropped.

Step 6. (Optional) To delete the configured tunnel mapping settings on a specific interface, enter the following:

Step 7. Enter the **end** command to go back to the Privileged EXEC mode:



```
[SG350X#configure
[SG350X(config)#interface ge1/0/48
[SG350X(config-if)#switchport vlan-mapping tunnel 30,40 10
[SG350X(config-if)#switchport vlan-mapping tunnel 50 drop
[SG350X(config-if)#end
 SG350X#
```

You should now have successfully configured the VLAN Tunnel Mapping settings on a specific port or ports on your switch through the CLI.

Configure One-to-One VLAN Mapping

In One-to-One VLAN Mapping, you can configure the C-VLAN ID entering the switch from the customer network and the assigned S-VLAN ID on a specific port on your switch. In the VLAN mapping One-to-One mode, an interface belongs to all S-VLANs for which mapping on this interface is defined as egress tagged interface. The interface PVID is set to 4095.

In the VLAN Mapping One-to-One mode, an interface uses one ingress ACL and one egress ACL. The One-to-One VLAN Mapping adds rules to these ACLs. These ACLs are applied in order to:

- Ingress ACL (in TTI):
- Replace specified C-VLAN-ID by S-VLAN-ID.
- Drop frames with unspecified C-VLAN-IDs.
- Drop untagged input frames.
- Egress ACL (in TCAM):
- Replace S-VLAN-ID by C-VLAN-ID.

The VLAN One-to-One mapping adds rules to these ACLs and they are bound on the interface only if its mode is VLAN Mapping One-to-One. The ingress ACL contains V+1 rules and the egress ACL contains V rules, where V is the number of specified C-VLANs.

Follow these steps to configure One-to-One VLAN mapping on a specific interface or interfaces of your switch:

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

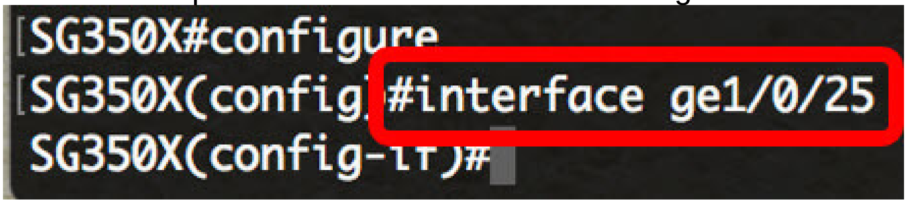
```
SG350X#configure
```

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

```
SG350X(config)#interface [interface-id]
```

The options are:

- interface-id - Specifies an interface ID to be configured.



```
SG350X#configure
SG350X(config)#interface ge1/0/25
SG350X(config-if)#
```

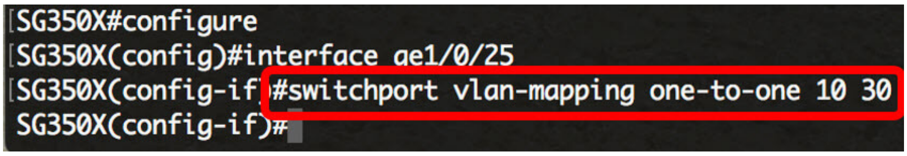
Note: In this example, interface ge1/0/25 is chosen.You can configure a few One-to-One VLAN Translation settings on the same interface.

Step 3. To configure one-to-one VLAN translation on an edge interface, enter the following:

```
SG350X(config-if)#switchport vlan-mapping one-to-one [vlan-id] [translated-vlan-id]
```

The parameters are:

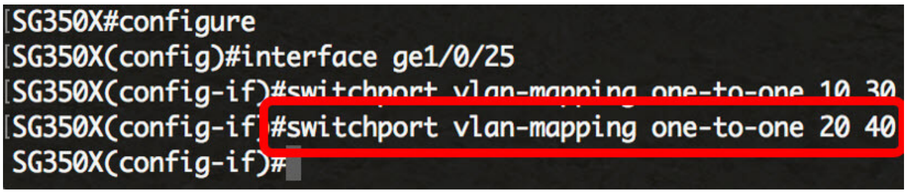
- vlan-id - Specifies the external VLAN (E-VLAN) for one-to-one VLAN translation. The range is from 1 to 4094.
- translated-vlan-id - Specifies B-VLAN replacing the E-VLAN. The range is from 1 to 4094.



```
[SG350X#configure
[SG350X(config)#interface ge1/0/25
[SG350X(config-if)#switchport vlan-mapping one-to-one 10 30
 SG350X(config-if)#
```

Note: In this example, VLAN 10 is entered as the Source VLAN and VLAN 30 is used as the Translated VLAN.

Step 4. (Optional) Repeat Step 3 to configure more One-to-One translation settings on the port or Steps 2 and 3 to configure other ports.

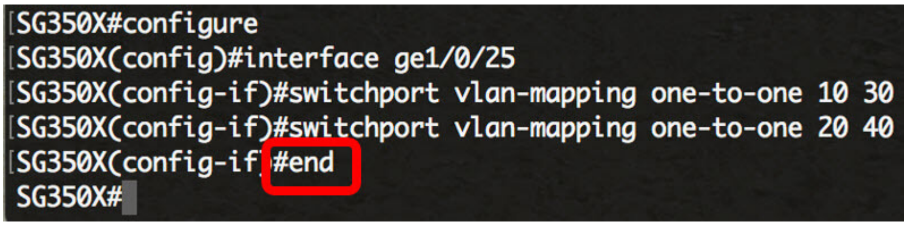


```
[SG350X#configure
[SG350X(config)#interface ge1/0/25
[SG350X(config-if)#switchport vlan-mapping one-to-one 10 30
[SG350X(config-if)#switchport vlan-mapping one-to-one 20 40
 SG350X(config-if)#
```

Note: In this example, new source and translated VLAN IDs are configured on the same GE25 interface.

Step 5. (Optional) To remove the configured one-to-one VLAN translation settings on the interface, enter the following:

Step 6. Enter the **end** command to go back to the Privileged EXEC mode:



```
[SG350X#configure
[SG350X(config)#interface ge1/0/25
[SG350X(config-if)#switchport vlan-mapping one-to-one 10 30
[SG350X(config-if)#switchport vlan-mapping one-to-one 20 40
[SG350X(config-if)#end
 SG350X#
```

You have now successfully configured the VLAN One-to-One mapping settings on a specific port or ports on your switch through the CLI.