



Configuring Asymmetric VLAN Mapping

This chapter describes how to configure the asymmetric VLAN mapping feature for Cisco Connected Grid switches. This chapter includes the following sections:

- [Supported Hardware, page 4-1](#)
- [Information About Asymmetric VLAN Mapping, page 4-1](#)
- [Default Settings, page 4-3](#)
- [Configuring Asymmetric VLAN Mapping, page 4-3](#)
- [Verifying Asymmetric VLAN Mapping Configuration, page 4-4](#)

Supported Hardware

Supported Hardware	Hardware Minimum Software Release	Related Documentation
Cisco CGS 2520 Switch	Cisco IOS Release 15.0(2)ED	Cisco 2500 Series Connected Grid Switches Configuration Guides

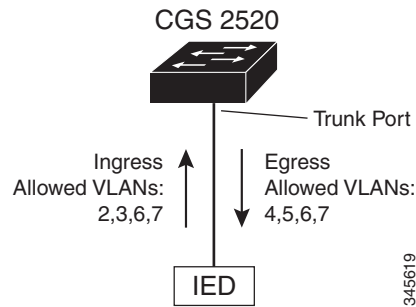
Information About Asymmetric VLAN Mapping

The asymmetric VLAN mapping feature for the Cisco CGS 2520 provides a method for restricting traffic on VLAN trunk ports. The feature lets you specify lists of VLANs that are allowed to forward traffic on the trunk port in the ingress direction, egress direction, or in both directions.

This feature is useful in a utility substation environment where a VLAN trunk is connected between a Cisco CGS 2520 switch and an intelligent electronic device (IED). The trunk port on the Cisco CGS 2520 can be configured to allow ingress traffic for a given VLAN, such as generic object oriented substation events (GOOSE) messages from the IED, and the trunk port can be configured to allow traffic for specific VLAN IDs in the egress direction, allowing the IED to subscribe to GOOSE messages with those VLAN IDs. All other VLAN traffic on the trunk port can be blocked.

In the example shown in [Figure 4-1](#), there are six VLANs (2, 3, 4, 5, 6, 7) configured on a Cisco CGS 2520 switch. Using the asymmetric VLAN mapping feature on a trunk port, packets tagged with VLANs 2 and 3 can only enter the system through that interface, packets tagged with VLANs 4 and 5 can only go out of the system (but cannot enter the system), and packets tagged with VLANs 6 and 7 can both enter and exit the system. Any other tagged packets are dropped at the interface level where this feature is configured.

Figure 4-1 Asymmetric VLAN Mapping Between a Cisco CGS 2520 and an IED



Configuration Guidelines

These are the guidelines for configuring asymmetric VLAN mapping:

- The asymmetric VLAN mapping feature is applicable only to Layer 2 trunk ports that are in NNI mode.
- The asymmetric VLAN mapping feature should only be configured on interfaces facing IEDs.
- The feature operates at the VLAN level, so it is applicable to all of the tagged frames received on the interface where the feature is configured. For non-tagged frames, native VLAN functionality is applied.
- VLANs must already exist on the switch prior to being included in the allowed ingress, egress, or bidirectional VLAN lists.
- The maximum number of VLANs that can be included in the allowed ingress, egress, or bidirectional VLAN lists for all interfaces on the switch is 945.
- If the ternary content addressable memory (TCAM) table on the switch is full, then it is not possible to configure asymmetric VLAN mapping.

Interaction with Other Features

The asymmetric VLAN mapping feature is configured on interfaces facing IEDs, so all other Layer 2 control protocols, such as Spanning Tree BPDUs, CDP, and VTP packets should not be exchanged between the interface and an attached IED.

When the asymmetric VLAN mapping feature is enabled on an interface, CDP, STP, and VTP are disabled and cannot be configured on the interface until any configuration statements for asymmetric VLAN mapping are removed. In addition, the **no switchport** and **switchport mode access** configuration statements are not allowed when configuration statements for asymmetric VLAN mapping are present on the interface.

When the asymmetric VLAN mapping feature is configured for an interface, the VLAN mapping feature (VLAN ID translation) and the allowed VLAN feature cannot be configured for that interface.

Default Settings

Parameters	Default
Asymmetric VLAN mapping feature on VLAN trunk ports	Disabled

Configuring Asymmetric VLAN Mapping

Beginning in privileged EXEC mode, follow these steps to configure asymmetric VLAN mapping:

	Command	Purpose
Step 1	<code>show vlan</code>	Verify that the VLANs for which you are configuring mapping rules exist on the switch. If not, create the VLANs on the switch.
Step 2	<code>interface type slot/port</code>	Specify the interface to be configured as the trunk interface, and enter interface configuration mode. The <i>type</i> can be fastethernet , gigabitethernet , or tengigabitethernet .
Step 3	<code>port-type nni</code>	Configure the interface as an NNI. Asymmetric VLAN mapping is supported only on NNI ports.
Step 4	<code>switchport mode trunk</code>	Configure the port as a trunk port.
Step 5	<code>switchport trunk allowed asymmetric-vlan bidirectional {add except none remove} vlan-list</code>	Specifies which of the VLANs configured on the switch are allowed to send traffic through the trunk port in both the ingress and egress directions. The add keyword adds VLANs to the current list. The except keyword indicates all VLANs except those specified by <i>vlan-list</i> . The none keyword specifies none of the VLANs. The remove keyword removes VLANs from the current list. The <i>vlan-list</i> parameter is either a single VLAN number from 1 to 4094; a range of VLANs described by two VLAN numbers, the lower one first, separated by a hyphen; or a comma-separated list of VLANs. Do not enter any spaces between comma-separated VLANs or in hyphen-specified ranges.
Step 6	<code>switchport trunk allowed asymmetric-vlan ingress {add except none remove} vlan-list</code>	Specifies which of the VLANs configured on the switch are allowed to send traffic through the trunk port in the ingress direction; that is, from the IED to the switch. Traffic coming into the trunk port from all other VLANs is blocked. See step 5 for the description of the add , except , none , remove , and <i>vlan-list</i> parameters.

Command	Purpose
Step 7 <code>switchport trunk allowed asymmetric-vlan egress {add except none remove} vlan-list</code>	Specifies which of the VLANs configured on the switch are allowed to send traffic through the trunk port in the egress direction; that is, from the switch to the IED. Traffic from all other VLANs is blocked from exiting the trunk port. See step 5 for the description of the add , except , none , remove , and <i>vlan-list</i> parameters.
Step 8 <code>no vtp</code>	Disable VTP. VTP cannot be configured on the same interface where asymmetric VLAN mapping is configured.
Step 9 <code>no cdp enable</code>	Disable CDP. CDP cannot be configured on the same interface where asymmetric VLAN mapping is configured.
Step 10 <code>exit</code>	Return to global configuration mode.

The following example shows how to configure asymmetric VLAN mapping for a Fast Ethernet port connected to an IED. The switch has six VLANs configured on it. A trunk port is configured on the Fast Ethernet port. Traffic for VLANs 6 and 7 is allowed in both the ingress and egress direction on the trunk port; traffic for VLANs 2 and 3 is allowed from the IED to the switch; traffic for VLANs 4 and 5 is allowed from the switch to the IED. Traffic from any other VLANs is blocked at the port.

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# port-type nni
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed asymmetric-vlan bidirectional 6,7
Switch(config-if)# switchport trunk allowed asymmetric-vlan ingress 2,3
Switch(config-if)# switchport trunk allowed asymmetric-vlan egress 4,5
Switch(config-if)# no vtp
Switch(config-if)# no cdp enable
Switch(config-if)# exit
```

Verifying Asymmetric VLAN Mapping Configuration

Command	Purpose
<code>show vlan asymmetric</code>	Display the asymmetric VLAN mapping configuration in summary