
# VLAN Configuration

This chapter describes how to configure normal-range VLANs (VLAN IDs 1 to 1005) and extended-range VLANs (VLAN IDs 1006 to 4094) on the CGR 2010 ESM. It includes information about VLAN membership modes, VLAN configuration modes, VLAN trunks, and dynamic VLAN assignment from a VLAN Membership Policy Server (VMPS).

**Note** For complete syntax and usage information for the commands used in this chapter, see the online *Cisco IOS Interface Command Reference, Release 12.2*.



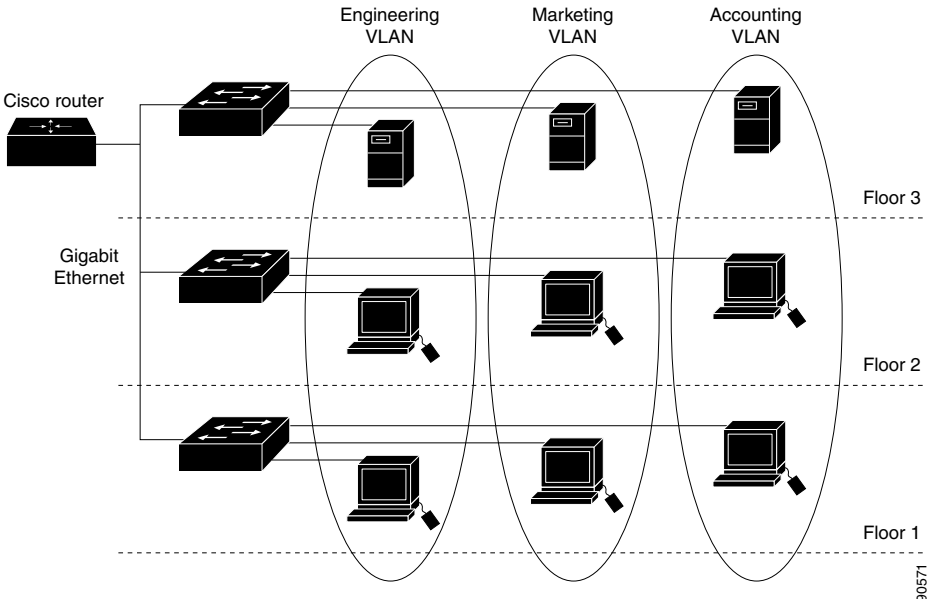
## Understanding VLANs

A VLAN is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment. Any switch module port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in the VLAN.

Each VLAN is considered a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a router, as shown in Figure 11-1. Because a VLAN is considered a separate logical network, it contains its own bridge MIB information and can support its own implementation of spanning tree. See Chapter 17, “Configuring STP” in the *Cisco CGS 2520 Software Configuration Guide*.

Figure 11-1 shows an example of VLANs segmented into logically defined networks.

***Figure 11-1 VLANs as Logically Defined Networks***




VLANs are often associated with IP subnetworks. For example, all the end stations in a particular IP subnet belong to the same VLAN. Interface VLAN membership on the switch module is assigned manually on an interface-by-interface basis. When you assign switch module interfaces to VLANs by using this method, it is known as interface-based, or static, VLAN membership.

**Note** The switch module does not support VLAN Trunking Protocol (VTP).

Traffic between VLANs must be routed. Switch modules that are running the IP services image can route traffic between VLANs by using Switch Virtual Interfaces (SVIs). To route traffic between VLANs, an SVI must be explicitly configured and assigned an IP address. For more information, see the "Switch Virtual Interfaces" section on page 8-5 and the "Configuring Layer 3 Interfaces" section on page 8-34.

This section includes these topics:



# Supported VLANs

VLANs are identified with a number from 1 to 4094. VLAN IDs 1002 through 1005 are reserved for Token Ring and FDDI VLANs. VLAN IDs greater than 1005 are extended-range VLANs and are not stored in the VLAN database.

Although the switch module supports a total of 1005 (normal-range and extended-range) VLANs, the number of routed ports, SVIs, and other configured features affects the use of the switch module hardware.

The switch module supports per-VLAN spanning-tree plus (PVST+) or rapid PVST+ with a maximum of 128 spanning-tree instances. One spanning-tree instance is allowed per VLAN.

**Note** Network node interfaces (NNIs) support STP by default. Enhanced network interfaces (ENIs) can be configured to support STP. User network interfaces (UNIs) do not support STP and by default are always in a forwarding state.

See the "VLAN Configuration Guidelines" section on page 11-8 for more information about the number of spanning-tree instances and the number of VLANs. The switch module supports IEEE 802.1Q trunking for sending VLAN traffic over Ethernet ports.

# Normal-Range VLANs

Normal-range VLANs are VLANs with VLAN IDs 1 to 1005. You can add, modify or remove configurations for VLANs 2 to 1001 in the VLAN database. (VLAN IDs 1 and 1002 to 1005 are automatically created and cannot be removed.)

Configurations for VLAN IDs 1 to 1005 are written to the file *vlan.dat* (VLAN database), and you can display them by entering the **show vlan** privileged EXEC command. The *vlan.dat* file is stored in flash memory.

**Caution** You can cause inconsistency in the VLAN database if you try to manually delete the *vlan.dat* file. If you want to modify the VLAN configuration, use the commands described in these sections and in the command reference for this release.

You can set these parameters when you create a new normal-range VLAN or modify an existing VLAN in the VLAN database:

- VLAN ID
- VLAN name
- VLAN type (Ethernet, Fiber Distributed Data Interface [FDDI], FDDI network entity title [NET], TrBRF, or TrCRF, Token Ring, Token Ring-Net)

**Note** The switch module supports only Ethernet VLANs. You can configure parameters for FDDI and Token Ring VLANs and view the results in the vlan.dat file, but these parameters are not used.

- VLAN state (active or suspended)
- Maximum transmission unit (MTU) for the VLAN
- Security Association Identifier (SAID)
- Bridge identification number for TrBRF VLANs
- Ring number for FDDI and TrCRF VLANs
- Parent VLAN number for TrCRF VLANs
- Spanning Tree Protocol (STP) type for TrCRF VLANs

- VLAN number to use when translating from one VLAN type to another
- Private VLAN. Configure the VLAN as a primary or secondary private VLAN. For information about private VLANs, see Chapter 12, "Private VLAN Configuration."
- Remote SPAN VLAN. Configure the VLAN as the Remote Switched Port Analyzer (RSPAN) VLAN for a remote SPAN session. For more information on remote SPAN, see Chapter 29, "Configuring SPAN and RSPAN" in the *CGS 2520 Software Configuration Guide*.
- UNI-ENI VLAN configuration

For extended-range VLANs, you can configure only MTU, private VLAN, remote SPAN VLAN, and UNI-ENI VLAN parameters.

**Note** This chapter does not provide configuration details for most of these parameters. For complete information on the commands and parameters that control VLAN configuration, see the command reference for this release.

# Extended-Range VLANs

You can create extended-range VLANs (in the range 1006 to 4094) to enable service providers to extend their infrastructure to a greater number of customers. The extended-range VLAN IDs are allowed for any **switchport** commands that allow VLAN IDs. Extended-range VLAN configurations are not stored in the VLAN database, but they are stored in the switch module running configuration file, and you can save the configuration in the startup configuration file by using the **copy running-config startup-config** privileged EXEC command.

**Note** Although the switch module supports 4094 VLAN IDs, the actual number of VLANs supported is 1005.

# VLAN Port Membership Modes

You configure a port to belong to a VLAN by assigning a membership mode that specifies the kind of traffic that the port carries and the number of VLANs to which it can belong. Table 11-1 lists the membership modes and characteristics.

***Table 11-1 Port Membership Modes***

| Membership Mode | VLAN Membership Characteristics |
|---|---|
| Static-access | A static-access port can belong to one VLAN and is manually assigned to that VLAN.<br>For more information, see the "Assigning Static-Access Ports to a VLAN" section on page 11-11. |
| Trunk (802.1Q) | A trunk port is a member of all VLANs by default, including extended-range VLANs, but membership can be limited by configuring the allowed-VLAN list.<br>For information about configuring trunk ports, see the "Configuring an Ethernet Interface as a Trunk Port" section on page 11-17. |

*Table 11-1 Port Membership Modes (continued)*

| Membership Mode | VLAN Membership Characteristics |
|---|---|
| Dynamic-access | A dynamic-access port can belong to one VLAN (VLAN ID 1 to 4094) and is dynamically assigned by a VMPS. The VMPS can be a Catalyst 5000 or Catalyst 6500 series switch, for example, but never a CGR 2010 ESM. The switch module is a VMPS client.<br>**Note** Only UNIs or ENIs can be dynamic-access ports.<br>You can have dynamic-access ports and trunk ports on the same switch module, but you must connect the dynamic-access port to an end station or hub and not to another switch module.<br>For configuration information, see the "Configuring Dynamic-Access Ports on VMPS Clients" section on page 11-27. |
| Private VLAN | A private VLAN port is a host or promiscuous port that belongs to a private VLAN primary or secondary VLAN. Only NNIs can be configured as promiscuous ports.<br>For information about private VLANs, see Chapter 12, "Configuring Private VLANs." |
| Tunnel (**dot1q-tunnel**) | Tunnel ports are used for 802.1Q tunneling to maintain customer VLAN integrity across a service-provider network. You configure a tunnel port on an edge switch module in the service-provider network and connect it to an 802.1Q trunk port on a customer interface, creating an assymetric link. A tunnel port belongs to a single VLAN that is dedicated to tunneling.<br>For more information about tunnel ports, see Chapter 13, "IEEE 802.1Q and Layer 2 Protocol Tunneling Configuration." |

For more detailed definitions of access and trunk modes and their functions, see Table 11-4 on page 11-16.

When a port belongs to a VLAN, the switch module learns and manages the addresses associated with the port on a per-VLAN basis.

# UNI-ENI VLANs

The CGR 2010 ESM is the boundary between customer networks and the service-provider network, with user network interfaces (UNIs) and enhanced interface interfaces (ENIs) connected to the customer side of the network. When customer traffic enters or leaves the service-provider network, the customer VLAN ID must be isolated from other customers' VLAN IDs. You can achieve this isolation by several methods, including using private VLANs. On the switch module, this isolation occurs by default by using UNI-ENI VLANs.

There are two types of UNI-ENI VLANs:

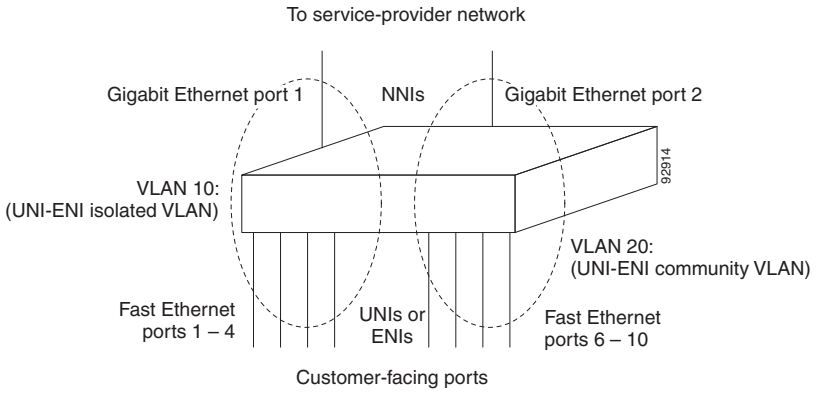
- UNI-ENI isolated VLAN—This is the default VLAN state for all VLANs created on the switch module. Local switching does not occur among UNIs or ENIs on the switch module that belong to the same UNI-ENI isolated VLAN. This configuration is designed for cases when different customers are connected to UNIs or ENIs on the same switch module. However, switching is allowed among UNIs or ENIs on different switches even though they belong to the same UNI-ENI isolated VLAN.
- UNI-ENI community VLAN—Local switching is allowed among UNIs and ENIs on the switch module that belong to the same community VLAN. If UNIs or ENIs belong to the same customer, and you want to switch module packets between the ports, you can configure the common VLAN as a UNI-ENI community VLAN. There is no local switching between the ports in a UNI-ENI community VLAN and ports outside of the VLAN. The switch module supports a combination of only eight UNIs and ENIs in a UNI-ENI community VLAN.

**Note** Local switching takes place between ENIs and UNIs in the same community VLAN. Because you can enable spanning tree on ENIs, but not on UNIs, you should use caution when configuring ENIs and UNIs in the same community VLAN. UNIs are always in the forwarding state.

Network node interfaces (NNIs) are not affected by the type of UNI-ENI VLAN to which they belong. Switching can occur between NNIs and other NNIs or UNIs or ENIs on the switch module or other switches that are part of the same VLAN, regardless of VLAN type.

In the configuration in Figure 11-2, if VLAN 10 is a UNI-ENI isolated VLAN and VLAN 20 is a UNI-ENI community VLAN, local switching does not take place among Fast Ethernet ports 1-4, but local switching can occur between Fast Ethernet ports 6-10. The NNIs in both VLAN 10 and VLAN 20 can exchange packets with the UNIs or ENIs in the same VLAN.

***Figure 11-2 UNI -ENI Isolated and Community VLANs in the Switch Module***




A UNI or ENI can be an access port, a trunk port, a private VLAN port, or an 802.1Q tunnel port. It can also be a member of an EtherChannel.

When a UNI or ENI configured as an 802.1Q trunk port belongs to a UNI-ENI isolated VLAN, the VLAN on the trunk is isolated from the same VLAN ID on a different trunk port or an access port. Other VLANs on the trunk port can be of different types (private VLAN, UNI-ENI community VLAN, and so on). For example, a UNI access port and one VLAN on a UNI trunk port can belong to the same UNI-ENI

isolated VLAN. In this case, isolation occurs between the UNI access port and the VLAN on the UNI trunk port. Other access ports and other VLANs on the trunk port are isolated because they belong to different VLANs.

UNIs, ENIs, and NNIs are always isolated from ports on different VLANs.

# Creating and Modifying VLANs

You use VLAN configuration mode, accessed by entering the **vlan** global configuration command to create VLANs and to modify some parameters. You use the interface configuration mode to define the port membership mode and to add and remove ports from VLANs. The results of these commands are written to the running-configuration file, and you can display the file by entering the **show running-config** privileged EXEC command.

These sections contain VLAN configuration information:



For more efficient management of the MAC address table space available on the switch module, you can control which VLANs learn MAC addresses by disabling MAC address learning on specific VLANs. See the"Disabling MAC Address Learning on a VLAN" section on page 6-32 for more information.

**Note** VLAN configuration is not recommended on FastEthernet ports FE0/9 to FE0/16 on the GRWIC-D-ES-2S-8PC (Copper model) and the FastEthernet ports FE0/5 to FE0/12 on the GRWIC-D-ES-6S (SFP model). For VLAN configuration on the backplane, we recommend using Port-channel48—see Chapter 9, "EtherChannel Configuration Between the Switch Module and the Host Router."

## Default Ethernet VLAN Configuration

The switch module supports only Ethernet interfaces. Table 11-2 shows the default configuration for Ethernet VLANs.

**Note** On extended-range VLANs, you can change only the MTU size, the private VLAN, the remote SPAN, and the UNI-ENI VLAN configuration. All other characteristics must remain at the default conditions.

*Table 11-2 Ethernet VLAN Defaults and Ranges*

| Parameter | Default | Range |
|---|---|---|
| VLAN ID | 1 | 1 to 4094.<br>**Note** Extended-range VLANs (VLAN IDs 1006 to 4094) are not saved in the VLAN database. |
| VLAN name | *VLANxxxx*, where *xxxx* represents four numeric digits (including leading zeros) equal to the VLAN ID number | No range |
| 802.10 SAID | 100001 (100000 plus the VLAN ID) | 1 to 4294967294 |
| MTU size | 1500 | 1500 to 9198 |
| Translational bridge 1 | 0 | 0 to1005 |
| Translational bridge 2 | 0 | 0 to1005 |
| VLAN state | active | active, suspend |
| Remote SPAN | disabled | enabled, disabled |
| Private VLANs | none configured | 2 to 1001, 1006 to 4094. |
| UNI-ENI VLAN | UNI-ENI isolated VLAN | 2 to 1001, 1006 to 4094.<br>VLAN 1 is always a UNI-ENI isolated VLAN. |

# VLAN Configuration Guidelines

Follow these guidelines when creating and modifying VLANs in your network:

- The switch module supports 1005 VLANs.
- Normal-range Ethernet VLANs are identified with a number between 1 and 1001. VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs.
- The switch module does not support Token Ring or FDDI media. The switch module does not forward FDDI, FDDI-Net, TrCRF, or TrBRF traffic.
- VLAN configurations for VLANs 1 to 1005 are always saved in the VLAN database and in the switch module running configuration file.
- Configuration options for VLAN IDs 1006 through 4094 (extended-range VLANs) are limited to MTU, RSPAN VLAN, private VLAN, and UNI-ENI VLAN. Extended-range VLANs are not saved in the VLAN database.
- Spanning Tree Protocol (STP) is enabled by default for only NNIs on all VLANs. You can configure STP on ENIs. NNIs and ENIs in the same VLAN are in the same spanning-tree instance. The switch module supports 128 spanning-tree instances. If a switch module has more active VLANs than supported spanning-tree instances, spanning tree can be enabled on 128 VLANs and is disabled on the remaining VLANs. If you have already used all available spanning-tree instances on a switch module, adding another VLAN creates a VLAN on that switch module that is not running spanning tree. If you have the default allowed list on the trunk ports of that switch module (which is to allow

all VLANs), the new VLAN is carried on all trunk ports. Depending on the topology of the network, this could create a loop in the new VLAN that would not be broken, particularly if there are several adjacent switches that all have run out of spanning-tree instances. You can prevent this possibility by setting allowed lists on the trunk ports of switches that have used up their allocation of spanning-tree instances.

If the number of VLANs on the switch module exceeds the number of supported spanning-tree instances, we recommend that you configure the 802.1s Multiple STP (MSTP) on your switch module to map multiple VLANs to a single spanning-tree instance.

**Note** MSTP is supported only on NNIs on ENIs on which STP has been enabled.

- Each routed port on the switch module creates an internal VLAN for its use. These internal VLANs use extended-range VLAN numbers, and the internal VLAN ID cannot be used for an extended-range VLAN. If you try to create an extended-range VLAN with a VLAN ID that is already allocated as an internal VLAN, an error message is generated, and the command is rejected.
  - Because internal VLAN IDs are in the lower part of the extended range, we recommend that you create extended-range VLANs beginning from the highest number (4094) and moving to the lowest (1006) to reduce the possibility of using an internal VLAN ID.
  - Before configuring extended-range VLANs, enter the **show vlan internal usage** privileged EXEC command to see which VLANs have been allocated as internal VLANs.
  - If necessary, you can shut down the routed port assigned to the internal VLAN, which frees up the internal VLAN, and then create the extended-range VLAN and re-enable the port, which then uses another VLAN as its internal VLAN. See the Creating an Extended-Range VLAN with an Internal VLAN ID, page 11-12.
- Although the switch module supports a total of 1005 (normal-range and extended-range) VLANs, the number of routed ports, SVIs, and other configured features affects the use of the switch module hardware. If you try to create an extended-range VLAN and there are not enough hardware resources available, an error message is generated, and the extended-range VLAN is rejected.

# Creating or Modifying an Ethernet VLAN

To access VLAN configuration mode, enter the **vlan** global configuration command with a VLAN ID. Enter a new VLAN ID to create a VLAN, or enter an existing VLAN ID to modify that VLAN. You can use the default VLAN configuration (Table 11-2) or enter commands to configure the VLAN.

**Note** Extended-range VLANs use the default Ethernet VLAN characteristics and the MTU, the private VLAN, the RSPAN, and the UNI-ENI VLAN configurations are the only parameters you can change.

For more information about commands available in this mode, see the **vlan** command description in the command reference for this release. When you have finished the configuration, you must exit VLAN configuration mode for the configuration to take effect. To display the VLAN configuration, enter the **show vlan** privileged EXEC command.

The configurations of VLAN IDs 1 to 1005 are always saved in the VLAN database (vlan.dat file) with a VLAN number and name and in the switch module running configuration file. Extended-range VLANs are not saved in the VLAN database; they are saved in the switch module running configuration file. You can save the VLAN configuration in the switch module startup configuration file by using the **copy running-config startup-config** privileged EXEC command.

**Note** Before you create an extended-range VLAN, you can verify that the VLAN ID is not used internally by entering the **show vlan internal usage** privileged EXEC command. If the VLAN ID is used internally and you want to release it, go to the Creating an Extended-Range VLAN with an Internal VLAN ID, page 11-12 before creating the extended-range VLAN.

Beginning in privileged EXEC mode, follow these steps to create or modify an Ethernet VLAN:

| | Step | Command |
|---|---|---|
| **Step 1** | Enter global configuration mode. | **configure terminal** |
| **Step 2** | Enter a VLAN ID, and enter VLAN configuration mode. Enter a new VLAN ID to create a VLAN, or enter an existing VLAN ID to modify that VLAN. The available VLAN ID range for this command is 1 to 4094.<br>**Note** When you create a new VLAN, by default the VLAN is a UNI-ENI isolated VLAN. | **vlan** *vlan-id* |
| **Step 3** | (Optional and supported on normal-range VLANs only) Enter a name for the VLAN. If no name is entered for the VLAN, the default in the VLAN database is to append the *vlan-id* with leading zeros to the word VLAN. For example, VLAN0004 is a default VLAN name for VLAN 4. | **name** *vlan-name* |
| **Step 4** | (Optional) Change the MTU size. | **mtu** *mtu-size* |
| **Step 5** | Return to privileged EXEC mode. | **end** |
| **Step 6** | Verify your entries. The **name** option is only valid for VLAN IDs 1 to 1005. | **show vlan** {**name** *vlan-name* \| **id** *vlan-id*} |
| **Step 7** | (Optional) Save the configuration in the switch module startup configuration file. | **copy running-config startup config** |

To delete a VLAN, use the **no vlan** *vlan-id* global configuration command. You cannot delete VLAN 1 or VLANs 1002 to 1005.

**Caution** When you delete a VLAN, any ports assigned to that VLAN become inactive. They remain associated with the VLAN (and inactive) until you assign them to a new VLAN.

To return the VLAN name to the default settings, use the **no name** or **no mtu** VLAN configuration command.

This example shows how to create Ethernet VLAN 20, name it *test20*, and add it to the VLAN database:

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# name test20
Switch(config-vlan)# end
```

This example shows how to create a new extended-range VLAN with all default characteristics, enter config-vlan mode, and save the new VLAN in the switch module startup configuration file:

```
Switch(config)# vlan 2000
Switch(config-vlan)# end
Switch# copy running-config startup config
```

# Assigning Static-Access Ports to a VLAN

You can assign a static-access port to a VLAN.

**Note** If you assign an interface to a VLAN that does not exist, the new VLAN is created. (See the "Creating or Modifying an Ethernet VLAN" section on page 11-9.)

Beginning in privileged EXEC mode, follow these steps to assign a port to a VLAN in the VLAN database:

| | Step | Command |
|---|---|---|
| **Step 1** | Enter global configuration mode | **configure terminal** |
| **Step 2** | Enter the interface to be added to the VLAN. | **interface** *interface-id* |
| **Step 3** | Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled. | **no shutdown** |
| **Step 4** | Define the VLAN membership mode for the port (Layer 2 access port). | **switchport mode access** |
| **Step 5** | Assign the port to a VLAN. Valid VLAN IDs are 1 to 4094. | **switchport access vlan** *vlan-id* |
| **Step 6** | Return to privileged EXEC mode. | **end** |
| **Step 7** | Verify the VLAN membership mode of the interface. | **show running-config interface** *interface-id* |
| **Step 8** | Verify your entries in the *Administrative Mode* and the *Access Mode VLAN* fields of the display. | **show interfaces** *interface-id* **switchport** |
| **Step 9** | (Optional) Save your entries in the configuration file. | **copy running-config startup-config** |

To return an interface to its default configuration, use the **default interface** *interface-id* interface configuration command.

This example shows how to configure a port as an access port in VLAN 2:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 2
Switch(config-if)# end
```

# Creating an Extended-Range VLAN with an Internal VLAN ID

If you enter an extended-range VLAN ID that is already assigned to an internal VLAN, an error message appears, and the extended-range VLAN is rejected. To manually release an internal VLAN ID, you must temporarily shut down the routed port that is using the internal VLAN ID.

Beginning in privileged EXEC mode, follow these steps to release a VLAN ID that is assigned to an internal VLAN and to create an extended-range VLAN with that ID:

| | Step | Command |
|---|---|---|
| **Step 1** | Display the VLAN IDs being used internally by the switch module. If the VLAN ID that you want to use is an internal VLAN, the display shows the routed port that is using the VLAN ID. Enter that port number in Step 3. | **show vlan internal usage** |
| **Step 2** | Enter global configuration mode. | **configure terminal** |
| **Step 3** | Specify the interface ID for the routed port that is using the VLAN ID, and enter interface configuration mode. | **interface** *interface-id* |
| **Step 4** | Shut down the port to release the internal VLAN ID. | **shutdown** |
| **Step 5** | Return to global configuration mode. | **exit** |
| **Step 6** | Enter the new extended-range VLAN ID, and enter config-vlan mode. | **vlan** *vlan-id* |
| **Step 7** | Exit from config-vlan mode, and return to global configuration mode. | **exit** |
| **Step 8** | Specify the interface ID for the routed port that you shut down in Step 4, and enter interface configuration mode. | **interface** *interface-id* |
| **Step 9** | Re-enable the routed port. It will be assigned a new internal VLAN ID. | **no shutdown** |
| **Step 10** | Return to privileged EXEC mode. | **end** |
| **Step 11** | (Optional) Save your entries in the switch module startup configuration file. | **copy running-config startup config** |

# Configuring UNI-ENI VLANs

By default, every VLAN configured on the switch module is a UNI-ENI isolated VLAN. You can change VLAN configuration to that of a UNI-ENI community VLAN, a private VLAN. or an RSPAN VLAN. You can also change the configuration of one of these VLANs to the default of a UNI-ENI isolated VLAN.

## Configuration Guidelines

These are the guidelines for UNI-ENI VLAN configuration:

- UNI-ENI isolated VLANs have no effect on NNI ports.

- A UNI-ENI community VLAN is like a traditional VLAN except that it can include no more than a combination of eight UNIs and ENIs.
- To change a VLAN type, first enter the **vlan** *vlan-id* global configuration command to enter VLAN configuration mode:
  - To change a VLAN from UNI-ENI isolated VLAN to a private VLAN, enter the **private-vlan** VLAN configuration command.
  - To change a UNI-ENI community VLAN to a private VLAN, you must first remove the community VLAN type by entering the **no uni-vlan** VLAN configuration command. Then enter the **private-vlan** VLAN configuration command.
  - To change a VLAN from a UNI-ENI isolated VLAN to an RSPAN VLAN, enter the **rspan-vlan** VLAN configuration command.
  - To change a UNI-ENI community VLAN to an RSPAN VLAN, you must first remove the community VLAN type by entering the **no uni-vlan** VLAN configuration command. Then enter the **rspan-vlan** VLAN configuration command.
  - To change a private VLAN to a UNI-ENI VLAN, you must first remove the private VLAN type by entering the **no private-vlan** VLAN configuration command. Then enter the **uni-vlan** VLAN configuration command.
  - To change an RSPAN VLAN to a UNI-ENI VLAN, you must first remove the RSPAN VLAN type by entering the **no rspan-vlan** VLAN configuration command. Then enter the **uni-vlan** VLAN configuration command
- The switch module supports a total of eight UNIs and ENIs in a community VLAN. You cannot configure a VLAN as a UNI-ENI community VLAN if more than eight UNIs and ENIs belong to the VLAN.
- If you attempt to add a UNI or ENI static access port to a UNI-ENI community VLAN that has a combination of eight UNIs and ENIs, the configuration is refused. If a UNI or ENI dynamic access port is added to a UNI-ENI community VLAN that has eight UNIs or ENIs, the port is error-disabled.
- Use caution when configuring ENIs and UNIs in the same community VLAN. Local switching takes place between the ENIs and UNIs in the community VLAN and ENIs can support spanning tree while UNIs do not.

## Configuring UNI-ENI VLANs

By default, every VLAN created on the switch module is a UNI-ENI isolated VLAN. You can change the configuration to UNI-ENI community VLAN or to a private VLAN or RSPAN VLAN. For procedures for configuring private VLANs, see Chapter 12, “Private VLAN Configuration.”

Beginning in privileged EXEC mode, follow these steps to change the type of a UNI-ENI VLAN:

| | Step | Command |
|---|---|---|
| **Step 1** | Enter global configuration mode. | **configure terminal** |
| **Step 2** | Enter a VLAN ID, and enter VLAN configuration mode. Enter a new VLAN ID to create a VLAN, or enter an existing VLAN ID to modify that VLAN. By default, the VLAN is a UNI-ENI isolated VLAN.<br>**Note** The available VLAN ID range for this command is 1 to 4094. | **vlan** *vlan-id* |
| **Step 3** | Configure the UNI-ENI VLAN type.<br>• Enter **community** to change from the default to a UNI-ENI community VLAN.<br>• Enter **isolated** to return to the default UNI-ENI isolated VLAN.<br>**Note** VLAN 1 is always a UNI-ENI isolated VLAN; you cannot configure VLAN 1 as a UNI-ENI community VLAN. The reserved VLANs 1002 to 1005 are not Ethernet VLANs. | **uni-vlan** {**community** \| **isolated**} |
| **Step 4** | Return to privileged EXEC mode. | **end** |
| **Step 5** | Display UNI-ENI VLAN information. Enter **type** (optional) to see only the VLAN ID and type of UNI-ENI VLAN. | **show vlan uni-vlan** [**type**] |
| **Step 6** | (Optional) Save the configuration in the switch module startup configuration file. | **copy running-config startup config** |

Use the **no uni-vlan** VLAN configuration command to return to the default (UNI-ENI isolated VLAN). Entering **uni-vlan isolated** command has the same effect as entering the no **uni-vlan** VLAN configuration command. The **show vlan** and **show vlan** *vlan-id* privileged EXEC commands also display UNI-ENI VLAN information, but only UNI-ENI community VLANs appear. To display both isolated and community VLANs, use the **show vlan uni-vlan type** command.

# Displaying VLANs

Use the **show vlan** privileged EXEC command to display a list of all VLANs on the switch module, including extended-range VLANs. The display includes VLAN status, ports, and configuration information. Table 11-3 lists other privileged EXEC commands for monitoring VLANs.

*Table 11-3 VLAN Monitoring Commands*

| Command | Description |
|---|---|
| **show interfaces** [**vlan** *vlan-id*] | Display characteristics for all interfaces or for the specified VLAN configured on the switch module. |
| **show vlan** [**id** *vlan-id*] | Display parameters for all VLANs or the specified VLAN on the switch module. |
| **show vlan** [*vlan-name*] **uni-vlan type** | Display UNI-ENI isolated or UNI-ENI community VLANs by VLAN name. |
| **show vlan uni-vlan** | Display UNI-ENI community VLANs and associated ports on the switch module. |
| **show vlan uni-vlan type** | Display UNI-ENI isolated and UNI-ENI community VLANs on the switch module by VLAN ID. |

For more details about the **show** command options and explanations of output fields, see the command reference for this release.

# Configuring VLAN Trunks



## Trunking Overview

A trunk is a point-to-point link between one or more Ethernet switch module interfaces and another networking device such as a router or a switch module. Ethernet trunks carry the traffic of multiple VLANs over a single link, and you can extend the VLANs across an entire network. The switch module supports the 802.1Q industry-standard trunking encapsulation.

You can configure a trunk on a single Ethernet interface or on an EtherChannel bundle.

Ethernet interfaces support different trunking modes (see Table 11-4). You can set an interface as trunking or nontrunking.

- If you do not intend to trunk across links, use the **switchport mode access** interface configuration command to disable trunking.

- To enable trunking, use the **switchport mode trunk** interface configuration command to change the interface to a trunk.

*Table 11-4 Layer 2 Interface Modes*

| Mode | Function |
|---|---|
| **switchport mode access** | Puts the interface (access port) into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The interface becomes a nontrunk interface regardless of whether or not the neighboring interface is a trunk interface. This is the default mode. |
| **switchport mode trunk** | Puts the interface into permanent trunking mode and negotiates to convert the neighboring link into a trunk link. The interface becomes a trunk interface even if the neighboring interface is not a trunk interface. |
| **switchport mode dot1q-tunnel** | Configures the interface as a tunnel (nontrunking) port to be connected in an asymmetric link with an 802.1Q trunk port. The 802.1Q tunneling is used to maintain customer VLAN integrity across a service provider network. See Chapter 13, "Configuring IEEE 802.1Q Tunneling," for more information on tunnel ports. |
| **switchport mode private-vlan** | Configure the interface as a private VLAN host or promiscuous port (only NNIs can be configured as promiscuous ports). For information about private VLANs, see Chapter 12, "Configuring Private VLANs." |

## IEEE 802.1Q Configuration Considerations

The 802.1Q trunks impose these limitations on the trunking strategy for a network:

- In a network of Cisco switches connected through 802.1Q trunks, the switches maintain one spanning-tree instance for each VLAN allowed on the trunks. Non-Cisco devices might support one spanning-tree instance for all VLANs.

  When you connect a Cisco switch module to a non-Cisco device through an 802.1Q trunk, the Cisco switch module combines the spanning-tree instance of the VLAN of the trunk with the spanning-tree instance of the non-Cisco 802.1Q switch module. However, spanning-tree information for each VLAN is maintained by Cisco switches separated by a cloud of non-Cisco 802.1Q switches. The non-Cisco 802.1Q cloud separating the Cisco switches is treated as a single trunk link between the switches.

- Make sure that the native VLAN for an 802.1Q trunk is the same on both ends of the trunk link. If the native VLAN on one end of the trunk is different from the native VLAN on the other end, spanning-tree loops might result.

- Disabling spanning tree on the native VLAN of an 802.1Q trunk without disabling spanning tree on every VLAN in the network can potentially cause spanning-tree loops. We recommend that you leave spanning tree enabled on the native VLAN of an 802.1Q trunk or disable spanning tree on every VLAN in the network. Make sure that your network is loop-free before disabling spanning tree.

# Default Layer 2 Ethernet Interface VLAN Configuration

Table 11-5 shows the default Layer 2 Ethernet interface VLAN configuration.

*Table 11-5 Default Layer 2 Ethernet Interface VLAN Configuration*

| Feature | Default Setting |
|---|---|
| Interface mode | **switchport mode access** |
| Allowed VLAN range | VLANs 1 to 4094 |
| Default VLAN (for access ports) | VLAN 1 |
| Native VLAN (for 802.1Q trunks) | VLAN 1 |

# Configuring an Ethernet Interface as a Trunk Port



## Interaction with Other Features

Trunking interacts with other features in these ways:

- A trunk port cannot be a secure port
- A trunk port cannot be a tunnel port
- Trunk ports can be grouped into EtherChannel port groups, but all trunks in the group must have the same configuration. When a group is first created, all ports follow the parameters set for the first port to be added to the group. If you change the configuration of one of these parameters, the switch module propagates the setting that you entered to all ports in the group:
  - allowed-VLAN list
  - STP port priority for each VLAN
  - STP Port Fast setting

**Note** STP is supported by default on NNIs, but must be enabled on ENIs. STP is not supported on UNIs.

  - trunk status: if one port in a port group ceases to be a trunk, all ports cease to be trunks.
- If you try to enable 802.1x on a trunk port, an error message appears, and 802.1x is not enabled. If you try to change the mode of an 802.1x-enabled port to trunk, the port mode is not changed.

## Configuring a Trunk Port

- Beginning in privileged EXEC mode, follow these steps to configure a port as an 802.1Q trunk port:

| | Step | Command |
|---|---|---|
| **Step 1** | Enter global configuration mode. | **configure terminal** |
| **Step 2** | Specify the port to be configured for trunking, and enter interface configuration mode. | **interface** *interface-id* |
| **Step 3** | Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled. | **no shutdown** |
| **Step 4** | Configure the interface as a Layer 2 trunk. | **switchport mode trunk** |
| **Step 5** | (Optional) Specify the default VLAN, which is used if the interface stops trunking. | **switchport access vlan** *vlan-id* |
| **Step 6** | Specify the native VLAN for 802.1Q trunks. | **switchport trunk native vlan** *vlan-id* |
| **Step 7** | Return to privileged EXEC mode. | **end** |
| **Step 8** | Display the switchport configuration of the interface in the *Administrative Mode* field of the display. | **show interfaces** *interface-id* **switchport** |
| **Step 9** | Display the trunk configuration of the interface. | **show interfaces** *interface-id* **trunk** |
| **Step 10** | (Optional) Save your entries in the configuration file. | **copy running-config startup-config** |

To return an interface to its default configuration, use the **default interface** *interface-id* interface configuration command. To reset all trunking characteristics of a trunking interface to the defaults, use the **no switchport trunk** interface configuration command. To disable trunking, use the **switchport mode access** interface configuration command to configure the port as a static-access port.

This example shows how to configure a port as an 802.1Q trunk with VLAN 33 as the native VLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface fastethernet0/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 33
Switch(config-if)# end
```

## Defining the Allowed VLANs on a Trunk

By default, a trunk port sends traffic to and receives traffic from all VLANs. All VLAN IDs, 1 to 4094, are allowed on each trunk. However, you can remove VLANs from the allowed list, preventing traffic from those VLANs from passing over the trunk. To restrict the traffic a trunk carries, use the **switchport trunk allowed vlan remove** *vlan-list* interface configuration command to remove specific VLANs from the allowed list.

**Note** VLAN 1 is the default VLAN on all trunk ports in all Cisco switches, and it has previously been a requirement that VLAN 1 always be enabled on every trunk link. The VLAN 1 minimization feature allows you to disable VLAN 1 on any individual VLAN trunk link so that no user traffic (including spanning-tree advertisements) is sent or received on VLAN 1. You do this by removing VLAN 1 from the allowed VLAN list.

To reduce the risk of spanning-tree loops or storms, you can disable VLAN 1 on any individual VLAN trunk port by removing VLAN 1 from the allowed list. When you remove VLAN 1 from a trunk port, the interface continues to send and receive management traffic, for example, Cisco Discovery Protocol (CDP), and Link Aggregation Control Protocol (LACP) in VLAN 1.

If a trunk port with VLAN 1 disabled is converted to a nontrunk port, it is added to the access VLAN. If the access VLAN is set to 1, the port is added to VLAN 1, regardless of the **switchport trunk allowed** setting. The same is true for any VLAN that has been disabled on the port.

A trunk port can become a member of a VLAN if the VLAN is enabled and if the VLAN is in the allowed list for the port.

Beginning in privileged EXEC mode, follow these steps to modify the allowed list of an IEEE 802.1Q trunk:

| | Step | Command |
|---|---|---|
| **Step 1** | Enter global configuration mode. | **configure terminal** |
| **Step 2** | Specify the port to be configured, and enter interface configuration mode. | **interface** *interface-id* |
| **Step 3** | Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled. | **no shutdown** |
| **Step 4** | Configure the interface as a VLAN trunk port. | **switchport mode trunk** |
| **Step 5** | (Optional) Configure the list of VLANs allowed on the trunk.<br>For explanations about using the **add**, **all**, **except**, and **remove** keywords, see the command reference for this release.<br>The *vlan-list* parameter is either a single VLAN number from 1 to 4094 or a range of VLANs described by two VLAN numbers, the lower one first, separated by a hyphen. Do not enter any spaces between comma-separated VLAN parameters or in hyphen-specified ranges.<br>All VLANs are allowed by default. | **switchport trunk allowed vlan** {**add** \| **all** \| **except** \| **remove**} *vlan-list* |
| **Step 6** | Return to privileged EXEC mode. | **end** |
| **Step 7** | Verify your entries in the *Trunking VLANs Enabled* field of the display. | **show interfaces** *interface-id* **switchport** |
| **Step 8** | (Optional) Save your entries in the configuration file. | **copy running-config startup-config** |

To return to the default allowed VLAN list of all VLANs, use the **no switchport trunk allowed vlan** interface configuration command.

This example shows how to remove VLAN 2 from the allowed VLAN list on a port:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport trunk allowed vlan remove 2
Switch(config-if)# end
```

## Configuring the Native VLAN for Untagged Traffic

A trunk port configured with 802.1Q tagging can receive both tagged and untagged traffic. By default, the switch module forwards untagged traffic in the native VLAN configured for the port. The native VLAN is VLAN 1 by default.

**Note** The native VLAN can be assigned any VLAN ID.

For information about 802.1Q configuration issues, see the "IEEE 802.1Q Configuration Considerations" section on page 11-16.

Beginning in privileged EXEC mode, follow these steps to configure the native VLAN on an IEEE 802.1Q trunk:

| | Step | Command |
|---|---|---|
| **Step 1** | Enter global configuration mode. | **configure terminal** |
| **Step 2** | Define the interface that is configured as the 802.1Q trunk, and enter interface configuration mode. | **interface** *interface-id* |
| **Step 3** | Enable the port, if necessary. By default, UNIs and ENIs are disabled and NNIs are enabled. | **no shutdown** |
| **Step 4** | Configure the VLAN that is sending and receiving untagged traffic on the trunk port.<br>For *vlan-id*, the range is 1 to 4094. | **switchport trunk native vlan** *vlan-id* |
| **Step 5** | Return to privileged EXEC mode. | **end** |
| **Step 6** | Verify your entries in the *Trunking Native Mode VLAN* field. | **show interfaces** *interface-id* **switchport** |
| **Step 7** | (Optional) Save your entries in the configuration file. | **copy running-config startup-config** |

To return to the default native VLAN, VLAN 1, use the **no switchport trunk native vlan** interface configuration command.

If a packet has a VLAN ID that is the same as the sending port native VLAN ID, the packet is sent untagged; otherwise, the switch module sends the packet with a tag.

# Configuring Trunk Ports for Load Sharing

Load sharing divides the bandwidth supplied by parallel trunks that connect switches. To avoid loops, STP normally blocks all but one parallel link between switches. Using load sharing, you divide the traffic between the links according to the VLAN to which the traffic belongs.

You configure load sharing on trunk ports that have STP enabled by using STP port priorities or STP path costs. For load sharing using STP port priorities, both load-sharing links must be connected to the same switch module. For load sharing using STP path costs, each load-sharing link can be connected to the same switch module or to two different switch modules.

## Load Sharing Using STP Port Priorities

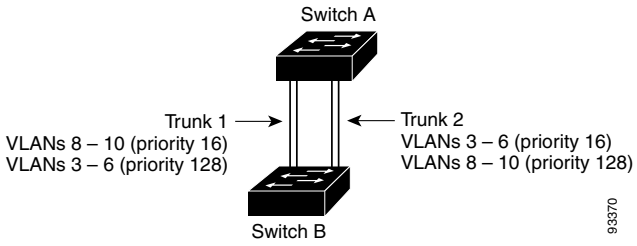
When two ports on the same switch module form a loop, the switch module uses the STP port priority to decide which port is enabled and which port is in a blocking state. You can set the priorities on a parallel STP trunk port so that the port carries all the traffic for a given VLAN. The trunk port with the higher priority (lower values) for a VLAN is forwarding traffic for that VLAN. The trunk port with the lower priority (higher values) for the same VLAN remains in a blocking state for that VLAN. One trunk port sends or receives all traffic for the VLAN.

Figure 11-3 shows two trunks connecting supported switches. In this example, the switches are configured as follows:

- VLANs 8 through 10 are assigned a port priority of 16 on Trunk 1
- VLANs 3 through 6 retain the default port priority of 128 on Trunk 1
- VLANs 3 through 6 are assigned a port priority of 16 on Trunk 2
- VLANs 8 through 10 retain the default port priority of 128 on Trunk 2

In this way, Trunk 1 carries traffic for VLANs 8 through 10, and Trunk 2 carries traffic for VLANs 3 through 6. If the active trunk fails, the trunk with the lower priority takes over and carries the traffic for all of the VLANs. No duplication of traffic occurs over any trunk port.

***Figure 11-3 Load Sharing by Using STP Port Priorities***




Beginning in privileged EXEC mode on Switch A, follow these steps to configure the network shown in Figure 11-3. Note that you can use any interface numbers; those shown are examples only.

| | Step | Command |
|---|---|---|
| **Step 1** | Verify that the referenced VLANs exist on Switch A. If not, create the VLANs by entering the VLAN IDs. | **show vlan** |
| **Step 2** | Enter global configuration mode. | **configure terminal** |

| | Step | Command |
|---|---|---|
| **Step 3** | Define the interface to be configured as the Trunk 1 interface, and enter interface configuration mode. | **interface gigabitethernet 0/1** |
| **Step 4** | Configure the interface as an NNI or ENI. UNIs do not support STP. If you configure the port as an ENI, you must also enable STP on the port by entering the **spanning-tree** interface configuration command. | **port-type** {**nni** \| **eni**} |
| **Step 5** | Configure the port as a trunk port. | **switchport mode trunk** |
| **Step 6** | Assign the port priority of 16 for VLANs 8 through 10 on Trunk 1. | **spanning-tree vlan 8-10 port-priority 16** |
| **Step 7** | Return to privileged EXEC mode. | **end** |
| **Step 8** | Verify the port configuration. | **show interfaces gigabitethernet 0/1 switchport** |
| **Step 9** | Enter global configuration mode. | **configure terminal** |
| **Step 10** | Define the interface to be configured as the Trunk 2 interface, and enter interface configuration mode. | **interface gigabitethernet 0/2** |
| **Step 11** | Configure the interface as an NNI or ENI. UNIs do not support STP. If you configure the port as an ENI, you must also enable STP on the port by entering the **spanning-tree** interface configuration command. | **port-type** {**nni** \| **eni**} |
| **Step 12** | Configure the port as a trunk port. | **switchport mode trunk** |
| **Step 13** | Assign the port priority of 16 for VLANs 3 through 6 on Trunk 2. | **spanning-tree vlan 3-6 port-priority 16** |
| **Step 14** | Return to privileged EXEC mode. | **end** |
| **Step 15** | Verify the port configuration. | **show interfaces gigabitethernet 0/2 switchport** |
| **Step 16** | Verify your entries. | **show running-config** |
| **Step 17** | (Optional) Save your entries in the configuration file. | **copy running-config startup-config** |

Follow the same steps on Switch B to configure the trunk port for Trunk 1 with a spanning-tree port priority of 16 for VLANs 8 through 10, and the configure trunk port for Trunk 2 with a spanning-tree port priority of 16 for VLANs 3 through 6.

## Load Sharing Using STP Path Cost

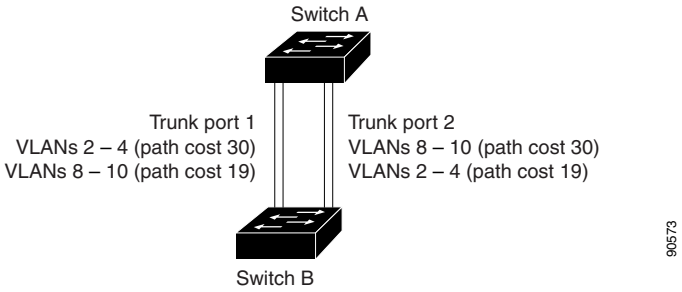
You can configure parallel trunks to share VLAN traffic by setting different path costs on a trunk and associating the path costs with different sets of VLANs, blocking different ports for different VLANs. The VLANs keep the traffic separate and maintain redundancy in the event of a lost link.

In Figure 11-4, Trunk ports 1 and 2 are configured as 100Base-T ports. These VLAN path costs are assigned:

- VLANs 2 through 4 are assigned a path cost of 30 on Trunk port 1

- VLANs 8 through 10 retain the default 100Base-T path cost on Trunk port 1 of 19
- VLANs 8 through 10 are assigned a path cost of 30 on Trunk port 2
- VLANs 2 through 4 retain the default 100Base-T path cost on Trunk port 2 of 19

***Figure 11-4 Load-Sharing Trunks with Traffic Distributed by Path Cost***




Beginning in privileged EXEC mode, follow these steps to configure the network shown in Figure 11-4:

| | Step | Command |
|---|---|---|
| **Step 1** | Enter global configuration mode on Switch A. | **configure terminal** |
| **Step 2** | Define the interface to be configured as Trunk port 1, and enter interface configuration mode. | **interface fastethernet0/1** |
| **Step 3** | Configure the interface as an NNI or ENI. UNIs do not support STP. If you configure the port as an ENI, you must also enable STP on the port by entering the **spanning-tree** interface configuration command. | **port-type** {**nni** \| **eni**} |
| **Step 4** | Configure the port as a trunk port. | **switchport mode trunk** |
| **Step 5** | Return to global configuration mode. | **exit** |
| **Step 6** | Define the interface to be configured as Trunk port 2, and enter interface configuration mode. | **interface fastethernet0/2** |
| **Step 7** | Configure the interface as an NNI or ENI. UNIs do not support STP. If you configure the port as an ENI, you must also enable STP on the port by entering the **spanning-tree** interface configuration command. | **port-type** {**nni** \| **eni**} |
| **Step 8** | Configure the port as a trunk port. | **switchport mode trunk** |
| **Step 9** | Return to privileged EXEC mode. | **end** |
| **Step 10** | Verify your entries. In the display, make sure that the interfaces configured in Steps 2 and 7 are configured as trunk ports. | **show running-config** |
| **Step 11** | Verify that VLANs 2 through 4 and 8 through 10 are configured on Switch A. If not, create these VLANs. | **show vlan** |
| **Step 12** | Enter global configuration mode. | **configure terminal** |
| **Step 13** | Enter interface configuration mode for Trunk port 2. | **interface fastethernet0/1** |

| | Step | Command |
|---|---|---|
| **Step 14** | Set the spanning-tree path cost to 30 for VLANs 2 through 4. | **spanning-tree vlan 2-4 cost 30** |
| **Step 15** | Return to global configuration mode. | **exit** |
| **Step 16** | Enter interface configuration mode for Trunk port 2. | **interface fastethernet0/2** |
| **Step 17** | Set the spanning-tree path cost to 30 for VLANs 2 through 4. | **spanning-tree vlan 8-10 cost 30** |
| **Step 18** | Return to global configuration mode. | **exit** |
| **Step 19** | Repeat Steps 9 through 11 on the other configured trunk interface on Switch A, and set the spanning-tree path cost to 30 for VLANs 8, 9, and 10. | |
| **Step 20** | Return to privileged EXEC mode. | **exit** |
| **Step 21** | Verify your entries. In the display, verify that the path costs are set correctly for both trunk interfaces. | **show running-config** |
| **Step 22** | (Optional) Save your entries in the configuration file. | **copy running-config startup-config** |

Follow the same steps on Switch B to configure the trunk port for Trunk 1 with a path cost of 30 for VLANs 2 through 4, and configure the trunk port for Trunk 2 with a path cost of 30 for VLANs 8 through 10.

# Configuring VMPS

The VLAN Query Protocol (VQP) supports dynamic-access ports, which are not permanently assigned to a VLAN, but give VLAN assignments based on the MAC source addresses seen on the port.

**Note** Only UNIs and ENIs can be configured as dynamic-access ports; NNIs cannot take part in VQP.

Each time an unknown MAC address is seen, the switch module sends a VQP query to a remote VMPS; the query includes the newly seen MAC address and the port on which it was seen. The VMPS responds with a VLAN assignment for the port. The switch module cannot be a VMPS server but can act as a client to the VMPS and communicate with it through VQP.

# Understanding VMPS

Each time the client switch module receives the MAC address of a new host, it sends a VQP query to the VMPS. When the VMPS receives this query, it searches its database for a MAC-address-to-VLAN mapping. The server response is based on this mapping and whether or not the server is in open or secure mode. In secure mode, the server shuts down the port when an illegal host is detected. In open mode, the server simply denies the host access to the port.

If the port is currently *unassigned* (that is, it does not yet have a VLAN assignment), the VMPS provides one of these responses:

- If the host is allowed on the port, the VMPS sends the client a *vlan-assignment* response containing the assigned VLAN name and allowing access to the host.
- If the host is not allowed on the port and the VMPS is in open mode, the VMPS sends an *access-denied* response.
- If the VLAN is not allowed on the port and the VMPS is in secure mode, the VMPS sends a *port-shutdown* response.

If the port already has a VLAN assignment, the VMPS provides one of these responses:

- If the VLAN in the database matches the current VLAN on the port, the VMPS sends an *success* response, allowing access to the host.
- If the VLAN in the database does not match the current VLAN on the port and active hosts exist on the port, the VMPS sends an *access-denied* or a *port-shutdown* response, depending on the secure mode of the VMPS.

If the switch module receives an *access-denied* response from the VMPS, it continues to block traffic to and from the host MAC address. The switch module continues to monitor the packets directed to the port and sends a query to the VMPS when it identifies a new host address. If the switch module receives a *port-shutdown* response from the VMPS, it disables the port. The port must be manually re-enabled by using the CLI or SNMP.

## Dynamic-Access Port VLAN Membership

A dynamic-access port can belong to only one VLAN with an ID from 1 to 4094. When the link comes up, the switch module does not forward traffic to or from this port until the VMPS provides the VLAN assignment. The VMPS receives the source MAC address from the first packet of a new host connected to the dynamic-access port and attempts to match the MAC address to a VLAN in the VMPS database.

**Note** Only UNIs or ENIs can be dynamic-access ports.

If there is a match, the VMPS sends the VLAN number for that port. If the client switch module was not previously configured, it uses the domain name from the first VTP packet it receives on its trunk port from the VMPS. If the client switch module was previously configured, it includes its domain name in the query packet to the VMPS to obtain its VLAN number. The VMPS verifies that the domain name in the packet matches its own domain name before accepting the request and responds to the client with the assigned VLAN number for the client. If there is no match, the VMPS either denies the request or shuts down the port (depending on the VMPS secure mode setting).

Multiple hosts (MAC addresses) can be active on a dynamic-access port if they are all in the same VLAN; however, the VMPS shuts down a dynamic-access port if more than 20 hosts are active on the port.

If the link goes down on a dynamic-access port, the port returns to an isolated state and does not belong to a VLAN. Any hosts that come online through the port are checked again through the VQP with the VMPS before the port is assigned to a VLAN.

Dynamic-access ports can be used for direct host connections, or they can connect to a network. A maximum of 20 MAC addresses are allowed per port on the switch module. A dynamic-access port can belong to only one VLAN at a time, but the VLAN can change over time, depending on the MAC addresses seen.

# Default VMPS Client Configuration

Table 11-6 shows the default VMPS and dynamic-access port configuration on client switches.

***Table 11-6 Default VMPS Client and Dynamic-Access Port Configuration***

| Feature | Default Setting |
|---|---|
| VMPS domain server | None |
| VMPS reconfirm interval | 60 minutes |
| VMPS server retry count | 3 |
| Dynamic-access ports | None configured |

# VMPS Configuration Guidelines

These guidelines and restrictions apply to dynamic-access port VLAN membership:

- You should configure the VMPS before you configure ports as dynamic-access ports.
- 802.1x ports cannot be configured as dynamic-access ports. If you try to enable 802.1x on a dynamic-access (VQP) port, an error message appears, and 802.1x is not enabled. If you try to change an 802.1x-enabled port to dynamic VLAN assignment, an error message appears, and the VLAN configuration is not changed.
- Trunk ports cannot be dynamic-access ports, but you can enter the **switchport access vlan dynamic** interface configuration command for a trunk port. In this case, the switch module retains the setting and applies it if the port is later configured as an access port.

  You must turn off trunking on the port before the dynamic-access setting takes effect.
- Dynamic-access ports cannot be monitor ports.
- Secure ports cannot be dynamic-access ports. You must disable port security on a port before it becomes dynamic.
- Private VLAN ports cannot be dynamic-access ports.
- Dynamic-access ports cannot be members of an EtherChannel group.
- Port channels cannot be configured as dynamic-access ports.

# Configuring the VMPS Client

You configure dynamic VLANs by using the VMPS (server). The switch module can be a VMPS client; it cannot be a VMPS server.

## Entering the IP Address of the VMPS

You must first enter the IP address of the server to configure the switch module as a client.

Beginning in privileged EXEC mode, follow these steps to enter the IP address of the VMPS:

| | Step | Command |
|---|---|---|
| **Step 1** | Enter global configuration mode. | **configure terminal** |
| **Step 2** | Enter the IP address of the switch module acting as the primary VMPS server. | **vmps server** *ipaddress* **primary** |
| **Step 3** | (Optional) Enter the IP address of the switch module acting as a secondary VMPS server.<br>You can enter up to three secondary server addresses. | **vmps server** *ipaddress* |
| **Step 4** | Return to privileged EXEC mode. | **end** |
| **Step 5** | Verify your entries in the *VMPS Domain Server* field of the display. | **show vmps** |
| **Step 6** | (Optional) Save your entries in the configuration file. | **copy running-config startup-config** |

**Note** You must have IP connectivity to the VMPS for dynamic-access ports to work. You can test for IP connectivity by pinging the IP address of the VMPS and verifying that you get a response.

## Configuring Dynamic-Access Ports on VMPS Clients

**Caution** Dynamic-access port VLAN membership is for end stations or hubs connected to end stations. Connecting dynamic-access ports to other switch modules can cause a loss of connectivity.

Beginning in privileged EXEC mode, follow these steps to configure a dynamic-access port on a VMPS client switch module:

| | Step | Command |
|---|---|---|
| **Step 1** | Enter global configuration mode. | **configure terminal** |
| **Step 2** | Specify the switch module port that is connected to the end station, and enter interface configuration mode. The port must be a UNI or an ENI. | **interface** *interface-id* |
| **Step 3** | Enable the port. | **no shutdown** |
| **Step 4** | Configure the port as a UNI or ENI. | **port-type** {**uni** \| **eni**} |
| **Step 5** | Set the port to access mode. | **switchport mode access** |

| | Step | Command |
|---|---|---|
| **Step 6** | Configure the port as eligible for dynamic VLAN membership.<br>The dynamic-access port must be connected to an end station. | **switchport access vlan dynamic** |
| **Step 7** | Return to privileged EXEC mode. | **end** |
| **Step 8** | Verify your entries in the *Operational Mode* field of the display. | **show interfaces** *interface-id* **switchport** |
| **Step 9** | (Optional) Save your entries in the configuration file. | **copy running-config startup-config** |

To return an interface to its default configuration, use the **default interface** *interface-id* interface configuration command. To reset the access mode to the default VLAN for the switch module, use the **no switchport access vlan** interface configuration command.

## Reconfirming VLAN Memberships

Beginning in privileged EXEC mode, follow these steps to confirm the dynamic-access port VLAN membership assignments that the switch module has received from the VMPS:

| | Step | Command |
|---|---|---|
| **Step 1** | Reconfirm dynamic-access port VLAN membership. | **vmps reconfirm** |
| **Step 2** | Verify the dynamic VLAN reconfirmation status. | **show vmps** |

## Changing the Reconfirmation Interval

VMPS clients periodically reconfirm the VLAN membership information received from the VMPS.You can set the number of minutes after which reconfirmation occurs.

Beginning in privileged EXEC mode, follow these steps to change the reconfirmation interval:

| | Step | Command |
|---|---|---|
| **Step 1** | Enter global configuration mode. | **configure terminal** |
| **Step 2** | Enter the number of minutes between reconfirmations of the dynamic VLAN membership. The range is 1 to 120. The default is 60 minutes. | **vmps reconfirm** *minutes* |
| **Step 3** | Return to privileged EXEC mode. | **end** |
| **Step 4** | Verify the dynamic VLAN reconfirmation status in the *Reconfirm Interval* field of the display. | **show vmps** |
| **Step 5** | (Optional) Save your entries in the configuration file. | **copy running-config startup-config** |

To return the switch module to its default setting, use the **no vmps reconfirm** global configuration command.

## Changing the Retry Count

Beginning in privileged EXEC mode, follow these steps to change the number of times that the switch module attempts to contact the VMPS before querying the next server:

| | Step | Command |
|---|---|---|
| **Step 1** | Enter global configuration mode. | **configure terminal** |
| **Step 2** | Change the retry count. The retry range is 1 to 10; the default is 3. | **vmps retry** *count* |
| **Step 3** | Return to privileged EXEC mode. | **end** |
| **Step 4** | Verify your entry in the *Server Retry Count* field of the display. | **show vmps** |
| **Step 5** | (Optional) Save your entries in the configuration file. | **copy running-config startup-config** |

To return the switch module to its default setting, use the **no vmps retry** global configuration command.

# Monitoring the VMPS

You can display information about the VMPS by using the **show vmps** privileged EXEC command. The switch module displays this information about the VMPS:

- VMPS VQP Version—the version of VQP used to communicate with the VMPS. The switch module queries the VMPS that is using VQP Version 1.
- Reconfirm Interval—the number of minutes the switch module waits before reconfirming the VLAN-to-MAC-address assignments.
- Server Retry Count—the number of times VQP resends a query to the VMPS. If no response is received after this many tries, the switch module starts to query the secondary VMPS.
- VMPS domain server—the IP address of the configured VLAN membership policy servers. The switch module sends queries to the one marked *current*. The one marked *primary* is the primary server.
- VMPS Action—the result of the most recent reconfirmation attempt. A reconfirmation attempt can occur automatically when the reconfirmation interval expired, or you can force it by entering the **vmps reconfirm** privileged EXEC command.

This is an example of output for the **show vmps** privileged EXEC command:

```
Switch# show vmps
VQP Client Status:
--------------------
VMPS VQP Version:   1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server: 172.20.128.86 (primary, current)
```

```
                    172.20.128.87
Reconfirmation status
---------------------
VMPS Action:         other
```

# Troubleshooting Dynamic-Access Port VLAN Membership

The VMPS shuts down a dynamic-access port under these conditions:

- The VMPS is in secure mode, and it does not allow the host to connect to the port. The VMPS shuts down the port to prevent the host from connecting to the network.
- More than 20 active hosts reside on a dynamic-access port

To disable and re-enable a disabled dynamic-access port, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command.

# VMPS Configuration Example

Figure 11-5 shows a network with a VMPS server switch module and VMPS client switch module with dynamic-access ports. In this example, these assumptions apply:

- The VMPS server and the VMPS client are separate switches
- The CGR 2010 ESM (Switch A) is the primary VMPS server
- The CGR 2010 ESM Switch C and Switch J are secondary VMPS servers
- End stations are connected to the clients, Switch B and Switch I
- The database configuration file is stored on the TFTP server with the IP address 172.20.22.7

*Figure 11-5 Dynamic Port VLAN Membership Configuration*