



CHAPTER 12

Configuring VLANs

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 Catalyst 2960 switch. 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 command reference for this release.

The chapter consists of these sections:

- [Understanding VLANs, page 12-1](#)
 - [Configuring Normal-Range VLANs, page 12-4](#)
 - [Configuring Extended-Range VLANs, page 12-11](#)
 - [Displaying VLANs, page 12-14](#)
 - [Configuring VLAN Trunks, page 12-14](#)
 - [Configuring VMPS, page 12-23](#)

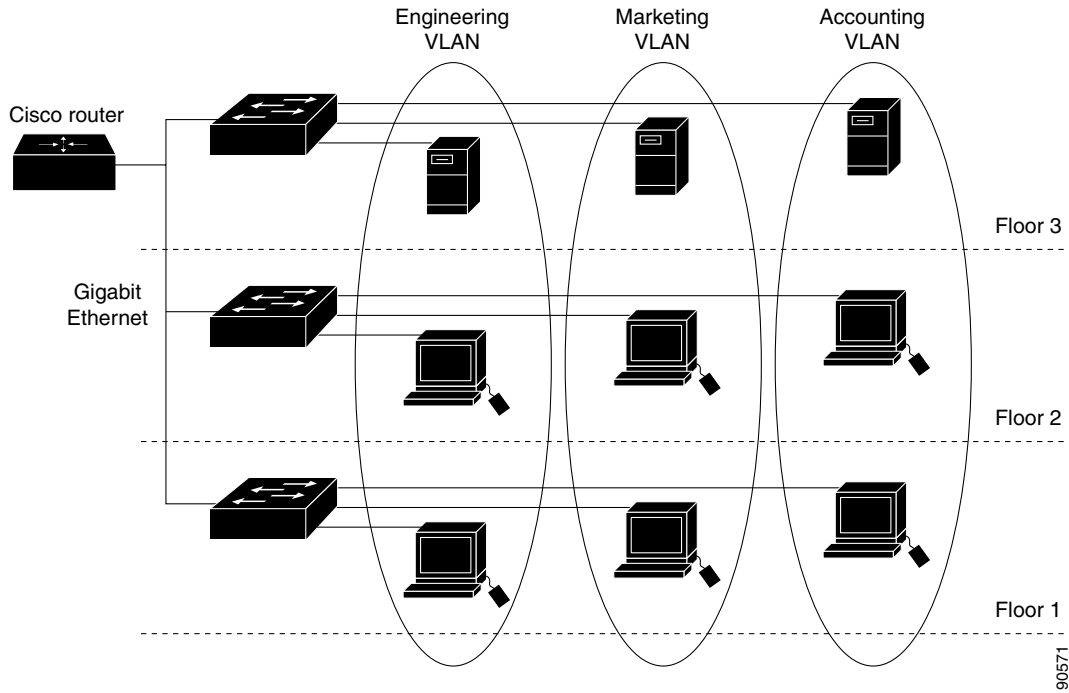
Understanding VLANs

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 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 or a switch supporting fallback bridging, as shown in [Figure 12-1](#). Because a VLAN is considered a separate logical network, it contains its own bridge Management Information Base (MIB) information and can support its own implementation of spanning tree. See [Chapter 15, “Configuring STP.”](#)



Before you create VLANs, you must decide whether to use VLAN Trunking Protocol (VTP) to maintain global VLAN configuration for your network. For more information on VTP, see [Chapter 13, “Configuring VTP.”](#)

Figure 12-1 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 is assigned manually on an interface-by-interface basis. When you assign switch interfaces to VLANs by using this method, it is known as interface-based, or static, VLAN membership.

Traffic between VLANs must be routed or fallback bridged.

Supported VLANs

VTP only learns normal-range VLANs, with VLAN IDs 1 to 1005; VLAN IDs greater than 1005 are extended-range VLANs and are not stored in the VLAN database. The switch must be in VTP transparent mode when you create VLAN IDs from 1006 to 4094.



Note

Up to 64 VLANs are supported when the switch is running the LAN Lite image.

Although the switch supports a total of 255 (normal range and extended range) VLANs, the number of configured features affects the use of the switch hardware.

The switch 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. See the [“Normal-Range VLAN Configuration Guidelines” section on page 12-5](#) for more information about the number of spanning-tree instances and the number of VLANs. The switch supports only IEEE 802.1Q trunking methods for sending VLAN traffic over Ethernet ports.



Note

VLAN Port Membership Modes

You configure a port to belong to a VLAN by assigning a membership mode that specifies the kind of traffic the port carries and the number of VLANs to which it can belong. [Table 12-1](#) lists the membership modes and membership and VTP characteristics.

Table 12-1 Port Membership Modes and Characteristics

Membership Mode	VLAN Membership Characteristics	VTP Characteristics
		VTP is not required. If you do not want VTP to globally propagate information, set the VTP mode to transparent. To participate in VTP, there must be at least one trunk port on the switch connected to a trunk port of a second switch.
Trunk (IEEE 802.1Q)	<p>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. You can also modify the pruning-eligible list to block flooded traffic to VLANs on trunk ports that are included in the list.</p> <p>For information about configuring trunk ports, see the “Configuring an Ethernet Interface as a Trunk Port” section on page 12-16.</p>	VTP is recommended but not required. VTP maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. VTP exchanges VLAN configuration messages with other switches over trunk links.
Dynamic access	<p>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 Catalyst 2960 switch. The Catalyst 2960 switch is a VMPS client.</p> <p>You can have dynamic-access ports and trunk ports on the same switch, but you must connect the dynamic-access port to an end station or hub and not to another switch.</p> <p>For configuration information, see the “Configuring Dynamic-Access Ports on VMPS Clients” section on page 12-26.</p>	<p>VTP is required.</p> <p>Configure the VMPS and the client with the same VTP domain name.</p> <p>To participate in VTP, at least one trunk port on the switch must be connected to a trunk port of a second switch.</p>
Voice VLAN	<p>A voice VLAN port is an access port attached to a Cisco IP Phone, configured to use one VLAN for voice traffic and another VLAN for data traffic from a device attached to the phone.</p> <p>For more information about voice VLAN ports, see Chapter 14, “Configuring Voice VLAN.”</p>	VTP is not required; it has no effect on a voice VLAN.

Configuring Normal-Range VLANs



Note

`show vlan` privileged EXEC command. The *vlan.dat* file is stored in flash memory.



Caution

`show running-config`

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

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



, page 12-7

[Default Ethernet VLAN Configuration, page 12-7](#)

[Creating or Modifying an Ethernet VLAN, page 12-8](#)

[Deleting a VLAN, page 12-10](#)

[Assigning Static-Access Ports to a VLAN, page 12-10](#)

Token Ring VLANs

-
-

Configuration Guide

Catalyst 5000 Series Software

Normal-Range VLAN Configuration Guidelines

-
-
-
-
-
-

VLAN Configuration Mode Options

-

vlan-id

database

VLAN Configuration in config-vlan Mode

VLAN Configuration in VLAN Database Configuration Mode

exit

apply exit

Saving VLAN Configuration

-
-
-



Caution

Default Ethernet VLAN Configuration



Note

Ethernet VLAN Defaults and Ranges

	Default	Range
		Note
	<i>VLANxxxx</i> <i>xxxx</i> (including leading zeros) equal to the VLAN ID number	No range
IEEE 802.10 SAID	100001 (100000 plus the VLAN ID)	1 to 4294967294
MTU size	1500	1500 to 18190

Ethernet VLAN Defaults and Ranges (continued)

Creating or Modifying an Ethernet VLAN



Note

Step 1	configure terminal	
Step 2		Note
Step 3	<i>vlan-name</i>	<i>vlan-id</i>
Step 4	<i>mtu-size</i>	
Step 5		
Step 6		Note

	Command	Purpose
Step 7	{ <i>vlan-name</i> <i>vlan-id</i> }	Verify your entries.
Step 8		

test20,

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



	Command	Purpose
Step 1		
Step 2		Note
Step 3		
Step 4		
Step 5		
Step 6		

```
vlan database
  vlan 20 name test20
  exit
APPLY completed.
Exiting...
```



	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		
Step 5		

Assigning Static-Access Ports to a VLAN



Note

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		
Step 5		
Step 6		
Step 7		<i>Administrative Mode Access Mode</i>
		<i>VLAN</i>

interface-id

Enter configuration commands, one per line. End with CNTL/Z.
 Switch(config)# **interface gigabitethernet0/1**
 switchport mode access
 switchport access vlan 2
 end

Configuring Extended-Range VLANs



Note



Extended-Range VLAN Configuration Guidelines

-
-
-
-
-
-
-

Displaying VLANs

Table 12-3 *VLAN Monitoring Commands*

Configuring VLAN Trunks

-
-
-
-

Trunking Overview

Protocol. However, some internetworking devices might forward DTP frames improperly, which could cause misconfigurations.



-
- `switchport nonegotiate`
- `switchport mode trunk`

Table 12-4 Layer 2 Interface Modes

	Function
	<i>trunk desirable</i>
	<i>trunk desirable auto</i>

IEEE 802.1Q Configuration Considerations

-
-
-

Default Layer 2 Ethernet Interface VLAN Configuration

Table 12-5 Default Layer 2 Ethernet Interface VLAN Configuration

	Default Setting

Configuring an Ethernet Interface as a Trunk Port

-
-
-
-

Interaction with Other Features

-
-

-
-
-
-

-
-

Configuring a Trunk Port

	Command	Purpose
Step 1		
Step 2		
Step 3	<pre> } } </pre>	<p>Configure the interface as a Layer 2 trunk (required only if the interface is a Layer 2 access port or to specify the trunking mode).</p> <ul style="list-style-type: none"> —Set the interface to a trunk link if the neighboring interface is set to trunk or desirable mode. This is the default. —Set the interface to a trunk link if the neighboring interface is set to trunk, desirable, or auto mode. —Set the interface in permanent trunking mode and negotiate to convert the link to a trunk link even if the neighboring interface is not a trunk interface.
		(Optional) Specify the default VLAN, which is used if the interface stops trunking.
		Specify the native VLAN for IEEE 802.1Q trunks.
		Return to privileged EXEC mode.
		Display the switchport configuration of the interface in the <i>show</i> command and the <i>Administrative Trunking Encapsulation</i> command.
Step 9	<pre> interface-id </pre>	

Defining the Allowed VLANs on a Trunk

vlan-list



Note

	Command	Purpose
Step 1		
Step 2	<i>interface-id</i>	
Step 3		
Step 4	<i>vlan-list</i>	<i>vlan-list</i>
Step 5		
Step 6	<i>interface-id</i>	<i>Trunking VLANs Enabled</i>
Step 7		

```
switchport trunk allowed vlan remove 2
end
```

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		
Step 5		<i>Pruning VLANs Enabled</i>

Configuring the Native VLAN for Untagged Traffic



Note



	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		
Step 5		
Step 6		

Load Sharing Using STP Port Priorities

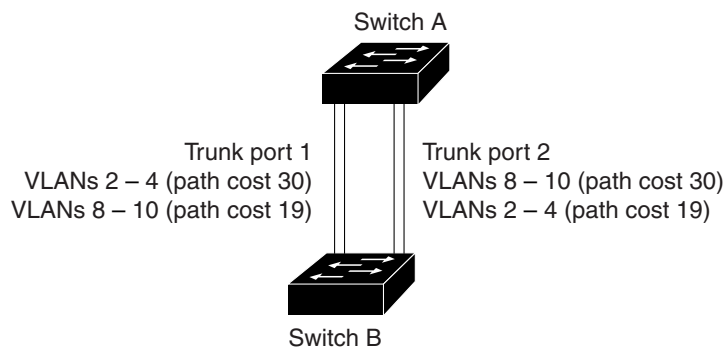
-
-



Step 16	<code>interface gigabitethernet 0/1</code>	
Step 17	<code>spanning-tree vlan 8-10 port-priority 16</code>	
	<code>exit</code>	
	<code>interface gigabitethernet0/2</code>	
	<code>spanning-tree vlan 3-6 port-priority 16</code>	
	<code>end</code>	
	<code>show running-config</code>	
	<code>copy running-config startup-config</code>	

Load Sharing Using STP Path Cost

-
-
-
-



<code>configure terminal</code>	
<code>interface gigabitethernet0/1</code>	
<code>switchport mode trunk</code>	

	Command	Purpose
Step 4		
Step 5		
Step 6		
Step 7		
Step 8		
Step 9		
Step 10		
Step 11	spanning-tree vlan 2-4 cost 30	
Step 12	end	
Step 13		
Step 14	exit	
Step 15	show running-config	
Step 16	copy running-config startup-config	

Configuring VMPS

-
-
-
-
-
-
-
-



Understanding VMPS

-
-
-

port-shutdown

success

access-denied port-shutdown

access-denied

port-shutdown

Dynamic-Access Port VLAN Membership

Default VMPS Client Configuration

Table 12-6 Default VMPS Client and Dynamic-Access Port Configuration

Feature	Default Setting

VMPS Configuration Guidelines

-
-
-
-
-
-
-
-
-
-

Configuring the VMPS Client

Entering the IP Address of the VMPS



Note

	Command	Purpose
Step 1		
Step 2		

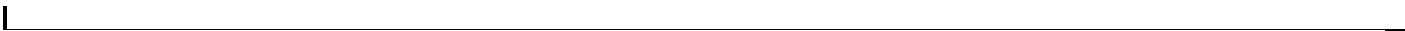


Note

Configuring Dynamic-Access Ports on VMPS Clients



Caution



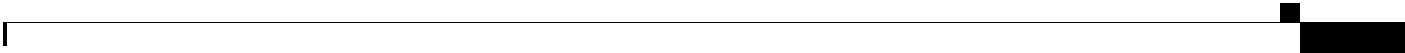
	Command	Purpose
Step 6		
Step 7		

Reconfirming VLAN Memberships

	Command	Purpose
Step 1		
Step 2		

Changing the Reconfirmation Interval

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		<i>Reconfirm Interval</i>



current

primary

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

The Catalyst 6500 series 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.

