CHAPTER 7

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 Cisco MWR 2941 router. It includes information about VLAN membership modes, VLAN configuration modes, and VLAN trunks.

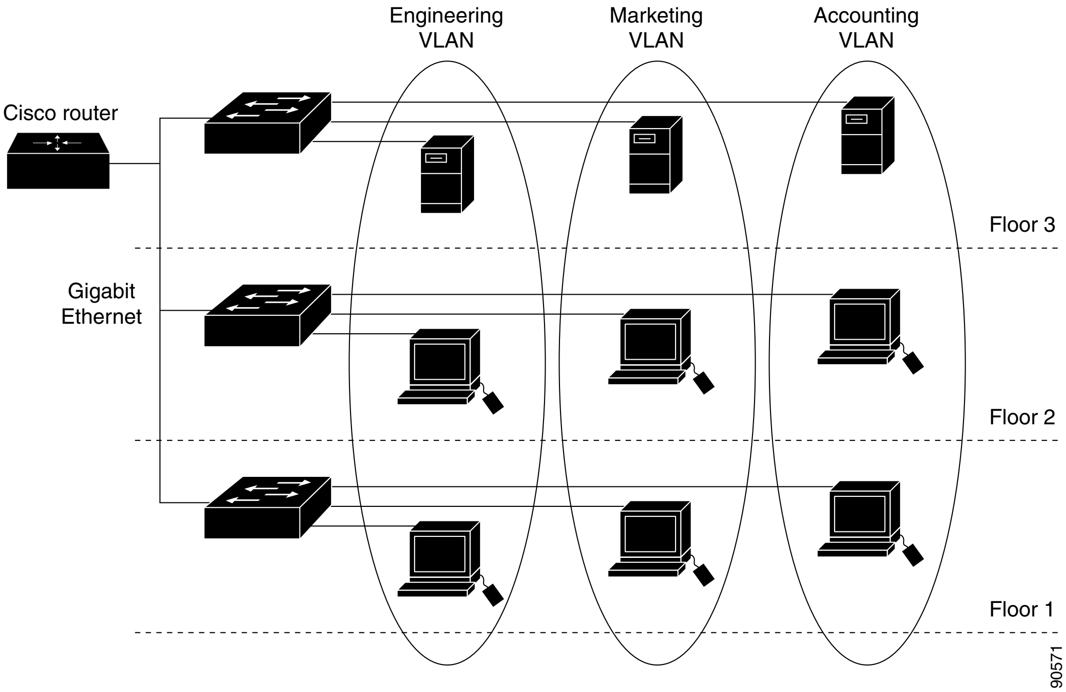
Note For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

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, as shown in Figure 7-1. 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 9, “Configuring STP.”

Figure 7-1 shows an example of VLANs segmented into logically defined networks.

Figure 7-1 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. Switches that are running the metro IP access 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 *Interface and Hardware Component Configuration Guide, Cisco IOS Release 15.0S.*.

This section includes these topics:

- Supported VLANs, page 7-2
- Normal-Range VLANs, page 7-3
- Extended-Range VLANs, page 7-4
- VLAN Port Membership Modes, page 7-4

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 router 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 hardware.

The router supports Per VLAN Spanning Tree Plus (PVST+) with a maximum of 128 spanning-tree instances. One spanning-tree instance is allowed per VLAN.

Note The router does not support Rapid PVST+.

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 7-6 for more information about the number of spanning-tree instances and the number of VLANs. The switch 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 this guide 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, FDDI, FDDI network entity title [NET], TrBRF, or TrCRF, Token Ring, Token Ring-Net)

Note The switch 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 ID (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

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 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 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 7-1 lists the membership modes and characteristics.

Table 7-1 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. For more information, see the "Assigning Static-Access Ports to a VLAN" section on page 7-8.
Trunk (IEEE 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. For information about configuring trunk ports, see the "Configuring an Ethernet Interface as a Trunk Port" section on page 7-13.
Tunnel (**dot1q-tunnel**)	Tunnel ports are used for IEEE 802.1Q tunneling to maintain customer VLAN integrity across a service-provider network. You configure a tunnel port on an edge switch in the service-provider network and connect it to an IEEE 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. For more information about tunnel ports, see Chapter 8, "Configuring IEEE 802.1Q Tunneling and Layer 2 Protocol Tunneling."

For more detailed definitions of access and trunk modes and their functions, see Table 7-4 on page 7-12.

When a port belongs to a VLAN, the switch learns and manages the addresses associated with the port on a per-VLAN basis. For more information, see the Chapter 12, "Managing the MAC Address Table.".

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:

- Default Ethernet VLAN Configuration, page 7-5
- VLAN Configuration Guidelines, page 7-6
- Creating or Modifying an Ethernet VLAN, page 7-7
- Assigning Static-Access Ports to a VLAN, page 7-8
- Creating an Extended-Range VLAN with an Internal VLAN ID, page 7-9

For more efficient management of the MAC address table space available on the switch, you can control which VLANs learn MAC addresses by disabling MAC address learning on specific VLANs. See the "Managing the MAC Address Table" section on page 12-1 for more information.

Default Ethernet VLAN Configuration

The switch supports only Ethernet interfaces. Table 7-2 shows the default configuration for Ethernet VLANs.

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

Table 7-2 Ethernet VLAN Defaults and Ranges

Parameter	Default	Range
VLAN ID	1	1–4094 **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
IEEE 802.10 SAID	100001 (100000 plus the VLAN ID)	1–4294967294
MTU size	1500	1500–9198
Translational bridge 1	0	0–1005
Translational bridge 2	0	0–1005

Table 7-2 Ethernet VLAN Defaults and Ranges (continued)

Parameter	Default	Range
VLAN state	active	active, suspend
UNI-ENI VLAN	UNI-ENI isolated VLAN	2–1001, 1006–4094 VLAN 1 is always a UNI-ENI isolated VLAN.

VLAN Configuration Guidelines

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

- The router 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 router does not support Token Ring or FDDI media. The switch 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 running configuration file.
- Configuration options for VLAN IDs 1006 through 4094 (extended-range VLANs) are limited to MTU. Extended-range VLANs are not saved in the VLAN database.
- STP is enabled by default only for 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 supports 128 spanning-tree instances. If a switch 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, adding another VLAN creates a VLAN on that switch that is not running spanning tree. If you have the default allowed list on the trunk ports of that switch (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 have run out of spanning-tree instances. You can prevent this 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 exceeds the number of supported spanning-tree instances, configure the IEEE 802.1s Multiple STP (MSTP) on your switch to map multiple VLANs to a single spanning-tree instance. For more information about MSTP, see Chapter 10, "Configuring MSTP."

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

- Each routed port on the switch 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" section on page 7-9.

- Although the switch 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 router 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 7-2) or enter commands to configure the VLAN.

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

For more information about commands available in VLAN configuration 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 running configuration file. Extended-range VLANs are not saved in the VLAN database; they are saved in the switch running configuration file. You can save the VLAN configuration in the switch 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" section on page 7-9 before creating the extended-range VLAN.

Follow these steps to create or modify an Ethernet VLAN:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vlan** *vlan-id*	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 1–4094. **Note** When you create a new VLAN, by default the VLAN is a UNI-ENI isolated VLAN.
Step 3	**name** *vlan-name*	(Optional and supported only on normal-range VLANs) 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.

	Command	Purpose
Step 4	**mtu** *mtu-size*	(Optional) Change the MTU size.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show vlan** {**name** *vlan-name* | **id** *vlan-id*}	Verify your entries. The **name** option is valid only for VLAN IDs 1 to 1005.
Step 7	**copy running-config startup config**	(Optional) Save the configuration in the switch startup configuration file.

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 thus 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:

```
Router# configure terminal
Router(config)# vlan 20
Router(config-vlan)# name test20
Router(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 startup configuration file:

```
Router(config)# vlan 2000
Router(config-vlan)# end
Router# 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 7-7.)

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

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode
Step 2	**interface** *interface-id*	Enter the interface to be added to the VLAN.
Step 3	**no shutdown**	Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled.
Step 4	**switchport mode access**	Define the VLAN membership mode for the port (Layer 2 access port).

	Command	Purpose
Step 5	**switchport access vlan** *vlan-id*	Assign the port to a VLAN. Valid VLAN IDs are 1 to 4094.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show running-config interface** *interface-id*	Verify the VLAN membership mode of the interface.
Step 8	**show interfaces** *interface-id* **switchport**	Verify your entries in the Administrative Mode and the Access Mode VLAN fields of the display.
Step 9	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

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:

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

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

Configuring VLAN Trunking Protocol

This section describes how to configure the VLAN Trunking Protocol (VTP) on an EtherSwitch HWIC, and contains the following tasks:

- Configuring a VTP Server
- Configuring a VTP Client
- Disabling VTP

Configuring a VTP Server

When a router is in VTP server mode, you can change the VLAN configuration and have it propagate throughout the network. Follow these steps to configure the router as a VTP server:

	Command	Purpose
Step 1	**enable**	Enter enable mode.
Step 2	**configure terminal**	Enter configuration mode.
Step 3	**vtp mode server**	Configure the router as a VTP server.
Step 4	**vtp domain**	Define the VTP domain name, which can be up to 32 characters long.
Step 5	**vtp password** *password*	(Optional) If you want to specify a password for the VTP domain, use **vtp password** command. The password can be from 8 to 64 characters long.
Step 6	**exit**	Exit configuration mode.

Configuring a VTP Client

When a router is in VTP client mode, you cannot change the VLAN configuration. A client switch receives VTP updates from a VTP server in the management domain and modifies its configuration accordingly. Follow these steps to configure the router as a VTP client.

	Command	Purpose
Step 1	**enable**	Enter enable mode.
Step 2	**configure terminal**	Enter configuration mode.
Step 3	**vtp mode client**	Configure the switch as a VTP client.
Step 4	**exit**	Exit configuration mode.

Disabling VTP

You can disable VTP on the router by configuring it to VTP transparent mode, meaning that the router does not send VTP updates or act on VTP updates received from other switches. Follow these steps to disable VTP on the router:

	Command	Purpose
Step 1	**enable**	Enter enable mode.
Step 2	**configure terminal**	Enter configuration mode.
Step 3	**vtp mode transparent**	Set the router in VTP transparent mode.
Step 4	**exit**	Exit configuration mode.

Note You can use the **show vtp status** command to verify the VTP status of the router.

Displaying VLANs

Use the **show vlan** privileged EXEC command to display a list of all VLANs on the router, including extended-range VLANs. The display includes VLAN status, ports, and configuration information. Table 7-3 lists other privileged EXEC commands for monitoring VLANs.

Table 7-3 VLAN Monitoring Commands

Command	Purpose
show interfaces [**vlan** *vlan-id*]	Display characteristics for all interfaces or for the specified VLAN configured on the router.
show vlan [**id** *vlan-id*]	Display parameters for all VLANs or the specified VLAN on the router.
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 router.
show vlan uni-vlan type	Display UNI-ENI isolated and UNI-ENI community VLANs on the router 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 interfaces and another networking device such as a router or a switch. Ethernet trunks carry the traffic of multiple VLANs over a single link, and you can extend the VLANs across an entire network. The router supports the IEEE 802.1Q industry-standard trunking encapsulation.

Ethernet interfaces support different trunking modes (see Table 7-4). 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 7-4 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 IEEE 802.1Q trunk port. The IEEE 802.1Q tunneling is used to maintain customer VLAN integrity across a service provider network. See Chapter 8, “Configuring IEEE 802.1Q Tunneling and Layer 2 Protocol Tunneling,” for more information on tunnel ports.

IEEE 802.1Q Configuration Considerations

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

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

- 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. Make sure that the native VLAN for an IEEE 802.1Q trunk is the same on both ends of the trunk link.
- Disabling spanning tree on the native VLAN of an IEEE 802.1Q trunk without disabling spanning tree on every VLAN in the network can potentially cause spanning-tree loops. Leave spanning tree enabled on the native VLAN of an IEEE 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 7-5 shows the default Layer 2 Ethernet interface VLAN configuration.

Table 7-5 Default Layer 2 Ethernet Interface VLAN Configuration

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

Configuring an Ethernet Interface as a Trunk Port

- Interaction with Other Features, page 7-13
- Defining the Allowed VLANs on a Trunk, page 7-14
- Configuring the Native VLAN for Untagged Traffic, page 7-15

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.
- If you try to enable IEEE 802.1x on a trunk port, an error message appears, and IEEE 802.1x is not enabled. If you try to change the mode of an IEEE 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 IEEE 802.1Q trunk port:

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

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 IEEE 802.1Q trunk with VLAN 33 as the native VLAN:

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

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:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the port to be configured, and enter interface configuration mode.
Step 3	**no shutdown**	Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled.
Step 4	**switchport mode trunk**	Configure the interface as a VLAN trunk port.
Step 5	**switchport trunk allowed vlan** {**add** | **all** | **except** | **remove**} *vlan-list*	(Optional) Configure the list of VLANs allowed on the trunk. For explanations about using the **add**, **all**, **except**, and **remove** keywords, see the command reference for this release. 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. All VLANs are allowed by default.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show interfaces** *interface-id* **switchport**	Verify your entries in the *Trunking VLANs Enabled* field of the display.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

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:

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

Configuring the Native VLAN for Untagged Traffic

A trunk port configured with IEEE 802.1Q tagging can receive both tagged and untagged traffic. By default, the router 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 IEEE 802.1Q configuration issues, see the "IEEE 802.1Q Configuration Considerations" section on page 7-12.

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

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

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 router 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. For load sharing using STP path costs, each load-sharing link can be connected to the same switch or to two different switches. For more information about STP, see Chapter 9, “Configuring STP.”

Load Sharing Using STP Port Priorities

When two ports on the same switch form a loop, the switch 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.

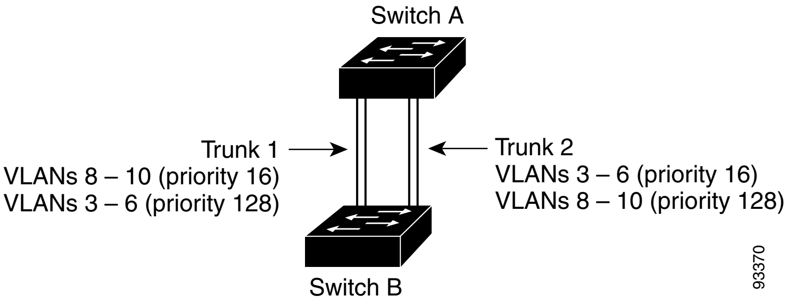
Figure 7-2 shows two trunks connecting supported switches. In this example, the switches are configured as follows:

- 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 7-2 Load Sharing by Using STP Port Priorities


Switch A
Trunk 1
VLANs 8 – 10 (priority 16)
VLANs 3 – 6 (priority 128)
Trunk 2
VLANs 3 – 6 (priority 16)
VLANs 8 – 10 (priority 128)
Switch B
93370

Beginning in privileged EXEC mode on Switch A, follow these steps to configure the network shown in Figure 7-2. Note that you can use any interface numbers; those shown are examples.

	Command	Purpose
Step 1	**show vlan**	Verify that the referenced VLANs exist on Switch A. If not, create the VLANs by entering the VLAN IDs.
Step 2	**configure terminal**	Enter global configuration mode.
Step 3	**interface gigabitethernet 0/1**	Define the interface to be configured as the Trunk 1 interface, and enter interface configuration mode.
Step 4	**switchport mode trunk**	Configure the port as a trunk port.
Step 5	**spanning-tree vlan 8-10 port-priority 16**	Assign the port priority of 16 for VLANs 8 through 10 on Trunk 1.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show interfaces gigabitethernet 0/1 switchport**	Verify the port configuration.
Step 8	**configure terminal**	Enter global configuration mode.
Step 9	**interface gigabitethernet 0/2**	Define the interface to be configured as the Trunk 2 interface, and enter interface configuration mode.
Step 10	**switchport mode trunk**	Configure the port as a trunk port.
Step 11	**spanning-tree vlan 3-6 port-priority 16**	Assign the port priority of 16 for VLANs 3 through 6 on Trunk 2.
Step 12	**end**	Return to privileged EXEC mode.
Step 13	**show interfaces gigabitethernet 0/2 switchport**	Verify the port configuration.
Step 14	**show running-config**	Verify your entries.
Step 15	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

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.

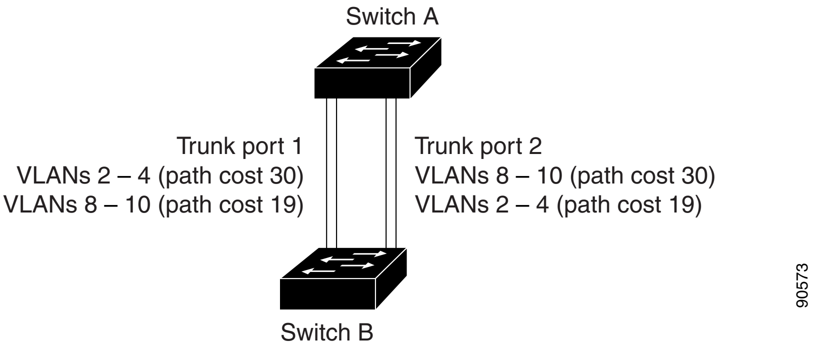
Load Sharing Using STP Path Cost

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 7-3, 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 7-3 Load-Sharing Trunks with Traffic Distributed by Path Cost


Switch A
Trunk port 1
VLANs 2 – 4 (path cost 30)
VLANs 8 – 10 (path cost 19)
Trunk port 2
VLANs 8 – 10 (path cost 30)
VLANs 2 – 4 (path cost 19)
Switch B
90573

Beginning in privileged EXEC mode, follow these steps to configure the network shown in Figure 7-3:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode on Switch A.
Step 2	**interface fastethernet0/1**	Define the interface to be configured as Trunk port 1, and enter interface configuration mode.
Step 3	**switchport mode trunk**	Configure the port as a trunk port.
Step 4	**exit**	Return to global configuration mode.
Step 5	**interface fastethernet0/2**	Define the interface to be configured as Trunk port 2, and enter interface configuration mode.
Step 6	**switchport mode trunk**	Configure the port as a trunk port.
Step 7	**end**	Return to privileged EXEC mode.
Step 8	**show running-config**	Verify your entries. In the display, make sure that the interfaces configured in Steps 2 and 7 are configured as trunk ports.
Step 9	**show vlan**	Verify that VLANs 2 through 4 and 8 through 10 are configured on Switch A. If not, create these VLANs.
Step 10	**configure terminal**	Enter global configuration mode.
Step 11	**interface fastethernet0/1**	Enter interface configuration mode for Trunk port 2.
Step 12	**spanning-tree vlan 2-4 cost 30**	Set the spanning-tree path cost to 30 for VLANs 2 through 4.

	Command	Purpose
Step 13	**exit**	Return to global configuration mode.
Step 14	**interface fastethernet0/2**	Enter interface configuration mode for Trunk port 2.
Step 15	**spanning-tree vlan 8-10 cost 30**	Set the spanning-tree path cost to 30 for VLANs 2 through 4.
Step 16	**exit**	Return to global configuration mode.
Step 17		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 18	**exit**	Return to privileged EXEC mode.
Step 19	**show running-config**	Verify your entries. In the display, verify that the path costs are set correctly for both trunk interfaces.
Step 20	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

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.