



## Creating and Maintaining VLANs

---

This chapter describes how to create and maintain VLANs. It includes information about VLAN modes, the VLAN Trunking Protocol (VTP) database, and the VLAN Membership Policy Server (VMPS).



**Note**

---

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 3550 Multilayer Switch Command Reference* for this release.

---

The chapter includes these sections:

- [Understanding VLANs, page 9-1](#)
- [Using the VLAN Trunking Protocol, page 9-3](#)
- [VLANs in the VTP Database, page 9-15](#)
- [Understanding VLAN Trunks, page 9-22](#)
- [Understanding VMPS, page 9-33](#)

## 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 bridge as shown in [Figure 9-1](#). 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 the Spanning Tree Protocol (STP).



**Note**

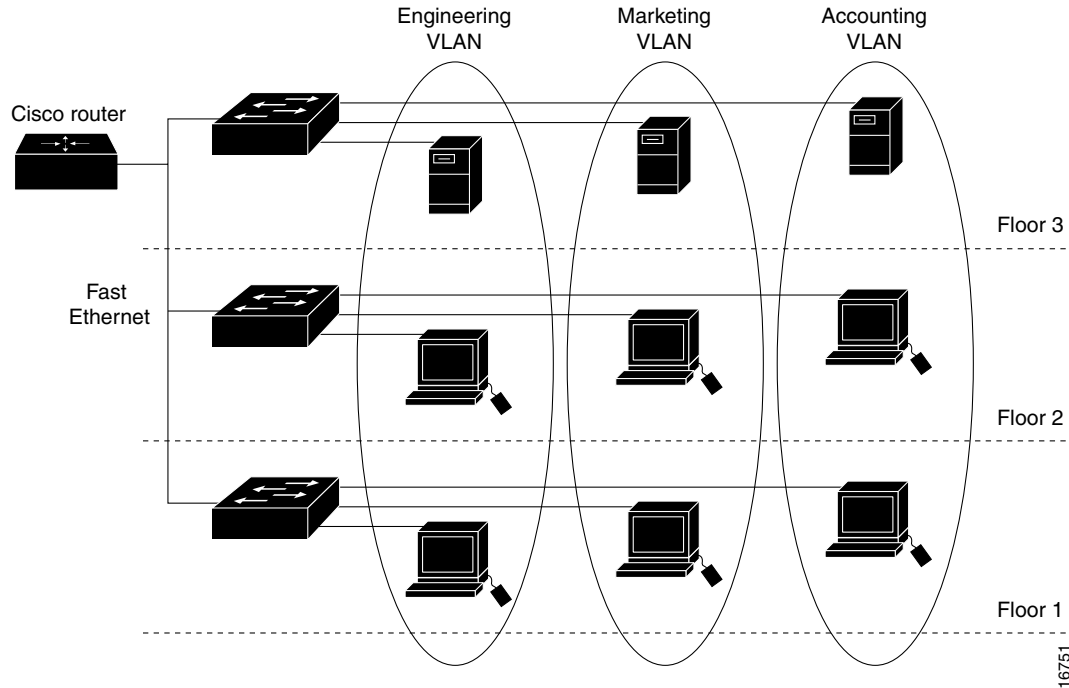
---

Before you create VLANs, you must decide whether to use VTP to maintain global VLAN configuration for your network. For more information on VTP, see the [“Using the VLAN Trunking Protocol” section on page 9-3](#).

---

[Figure 9-1](#) shows an example of VLANs segmented into logically defined networks.

Figure 9-1 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. A Catalyst 3550 switch with the enhanced multilayer software image installed can route traffic between VLANs by using switch virtual interfaces (SVIs). An SVI must be explicitly configured and assigned an IP address to route traffic between VLANs. For more information, see the [“Switch Virtual Interfaces”](#) section on page 8-4 and the [“Configuring Layer 3 Interfaces”](#) section on page 8-22.

## Number of Supported VLANs

The Catalyst 3550 switch supports 1005 VLANs in VTP client, server, and transparent modes. 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 supports per-VLAN spanning tree (PVST) with a maximum of 128 spanning-tree instances. One spanning-tree instance is allowed per VLAN.

The switch supports both Inter-Switch Link (ISL) and IEEE 802.1Q trunking methods for sending VLAN traffic over Ethernet ports.

## VLAN Port Membership Modes

You configure a port to belong to a VLAN by assigning a membership mode that determines the kind of traffic the port carries and the number of VLANs to which it can belong. [Table 9-1](#) lists the membership modes and characteristics.

**Table 9-1** Port Membership Modes

| Membership Mode            | VLAN Membership Characteristics  |
|----------------------------|--|
| Static-access              | <p>A static-access port can belong to one VLAN and is manually assigned by using the <b>switchport mode access</b> interface configuration command.</p> <p>For more information, see the <a href="#">“Assigning Static-Access Ports to a VLAN”</a> section on page 9-19.</p>   |
| Trunk (ISL or IEEE 802.1Q) | <p>A trunk is a member of all VLANs in the VLAN database by default, 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>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.</p> <p>Configure VLAN trunks using the <b>switchport mode trunk</b> interface configuration command. For more information, see the <a href="#">“Configuring an Ethernet Interface as a Trunk Port”</a> section on page 9-25.</p> |
| Dynamic access             | <p>A dynamic-access port can belong to one VLAN and is dynamically assigned by a VMPS. The VMPS can be a Catalyst 5000 or Catalyst 6000 series switch, for example, but never a Catalyst 3550 switch.</p> <p>You begin configuration by using the <b>switchport mode access</b> interface configuration command.</p> <p>For more information, see the <a href="#">“Configuring an Interface as a Layer 2 Dynamic Access Port”</a> section on page 9-37.</p>  |

For more detailed definitions of the modes and their functions, see [Table 9-6](#) on page 9-23.

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 [“Managing the MAC Address Table”](#) section on page 6-51.

## Using the VLAN Trunking Protocol

VTP is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. VTP minimizes misconfigurations and configuration inconsistencies that can cause several problems, such as duplicate VLAN names, incorrect VLAN-type specifications, and security violations.

Before you create VLANs, you must decide whether to use VTP in your network. Using VTP, you can make configuration changes centrally on one or more switches and have those changes automatically communicated to all the other switches in the network. Without VTP, you cannot send information about VLANs to other switches.

## The VTP Domain and VTP Modes

A VTP domain (also called a VLAN management domain) consists of one switch or several interconnected switches under the same administrative responsibility sharing the same VTP domain name. A switch can be in only one VTP domain. You make global VLAN configuration changes for the domain by using the command-line interface (CLI), Cluster Management Suite (CMS) software, or Simple Network Management Protocol (SNMP).

You can configure a supported switch to be in one of the VTP modes listed in [Table 9-2](#).

**Table 9-2 VTP Modes**

| VTP Mode        | Description   |
|-----------------|---|
| VTP server      | <p>In this mode, you can create, modify, and delete VLANs and specify other configuration parameters (such as the VTP version) for the entire VTP domain. VTP servers advertise their VLAN configurations to other switches in the same VTP domain and synchronize their VLAN configurations with other switches based on advertisements received over trunk links.</p> <p>In VTP server mode, VLAN configurations are saved in nonvolatile RAM (NVRAM). VTP server is the default mode.</p>  |
| VTP client      | <p>A VTP client behaves like a VTP server, but you cannot create, change, or delete VLANs on a VTP client.</p> <p>In VTP client mode, VLAN configurations are not saved in NVRAM.</p>   |
| VTP transparent | <p>VTP transparent switches do not participate in VTP. A VTP transparent switch does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. However, in VTP version 2, transparent switches do forward VTP advertisements that they receive from other switches from their trunk interfaces. You can create, modify, and delete VLANs on a switch in VTP transparent mode.</p> <p>In VTP transparent mode, VLAN configurations are saved in NVRAM, but they are not advertised to other switches.</p> |

By default, the switch is in VTP server mode and in the no-management-domain state until it receives an advertisement for a domain over a trunk link (a link that carries the traffic of multiple VLANs) or until you configure a domain name. Until the management domain name is specified or learned, you cannot create or modify VLANs on a VTP server, and VLAN information is not propagated over the network.

If the switch receives a VTP advertisement over a trunk link, it inherits the management domain name and the VTP configuration revision number. The switch then ignores advertisements with a different domain name or an earlier configuration revision number.

When you make a change to the VLAN configuration on a VTP server, the change is propagated to all switches in the VTP domain. VTP advertisements are sent over all trunk connections, including Inter-Switch Link (ISL) and IEEE 802.1Q.

VTP maps VLANs dynamically across multiple LAN types with unique names and internal index associates. Mapping eliminates excessive device administration required from network administrators.

If you configure a switch for VTP transparent mode, you can create and modify VLANs, but the changes are not sent to other switches in the domain, and they affect only the individual switch.

The [“Configuring VTP” section on page 9-8](#) provides tips and caveats for configuring VTP.

## VTP Advertisements

Each switch in the VTP domain sends periodic global configuration advertisements from each trunk port to a reserved multicast address. Neighboring switches receive these advertisements and update their VTP and VLAN configurations as necessary.

**Note**

---

Because trunk ports send and receive VTP advertisements, you must ensure that at least one trunk port is configured on the switch and that this trunk port is connected to the trunk port of a second switch. Otherwise, the switch cannot receive any VTP advertisements. For more information on trunk ports, see the [“Understanding VLAN Trunks” section on page 9-22](#).

---

VTP advertisements distribute this global domain information:

- VTP domain name
- VTP configuration revision number
- Update identity and update timestamp
- MD5 digest VLAN configuration, including maximum transmission unit (MTU) size for each VLAN.
- Frame format

VTP advertisements distribute this VLAN information for each configured VLAN:

- VLAN IDs (ISL and 802.1Q)
- VLAN name
- VLAN type
- VLAN state
- Additional VLAN configuration information specific to the VLAN type

## VTP Version 2

If you use VTP in your network, you must decide whether to use version 1 or version 2.

VTP version 2 supports these features not supported in version 1:

- Token Ring support—VTP version 2 supports Token Ring Bridge Relay Function (TrBRF) and Token Ring Concentrator Relay Function (TrCRF) VLANs. For more information about Token Ring VLANs, see the [“VLANs in the VTP Database” section on page 9-15](#).
- Unrecognized Type-Length-Value (TLV) support—A VTP server or client propagates configuration changes to its other trunks, even for TLVs it is not able to parse. The unrecognized TLV is saved in NVRAM when the switch is operating in VTP server mode.
- Version-Dependent Transparent Mode—In VTP version 1, a VTP transparent switch inspects VTP messages for the domain name and version and forwards a message only if the version and domain name match. Because VTP version 2 supports only one domain, it forwards VTP messages in transparent mode without inspecting the version and domain name.
- Consistency Checks—In VTP version 2, VLAN consistency checks (such as VLAN names and values) are performed only when you enter new information through the CLI, the Cluster Management Software (CMS), or SNMP. Consistency checks are not performed when new information is obtained from a VTP message or when information is read from NVRAM. If the MD5 digest on a received VTP message is correct, its information is accepted.

## VTP Pruning

VTP pruning increases network available bandwidth by restricting flooded traffic to those trunk links that the traffic must use to reach the destination devices. Without VTP pruning, a switch floods broadcast, multicast, and unknown unicast traffic across all trunk links within a VTP domain even though receiving switches might discard them. VTP pruning is disabled by default.

VTP pruning blocks unneeded flooded traffic to VLANs on trunk ports that are included in the pruning-eligible list. Only VLANs included in the pruning-eligible list can be pruned. By default, VLANs 2 through 1001 are pruning eligible on Catalyst 3550 trunk ports. If the VLANs are configured as pruning-ineligible, the flooding continues. VTP pruning is supported with VTP version 1 and version 2.

[Figure 9-2](#) shows a switched network without VTP pruning enabled. Port 1 on Switch 1 and Port 2 on Switch 4 are assigned to the Red VLAN. If a broadcast is sent from the host connected to Switch 1, Switch 1 floods the broadcast and every switch in the network receives it, even though Switches 3, 5, and 6 have no ports in the Red VLAN.

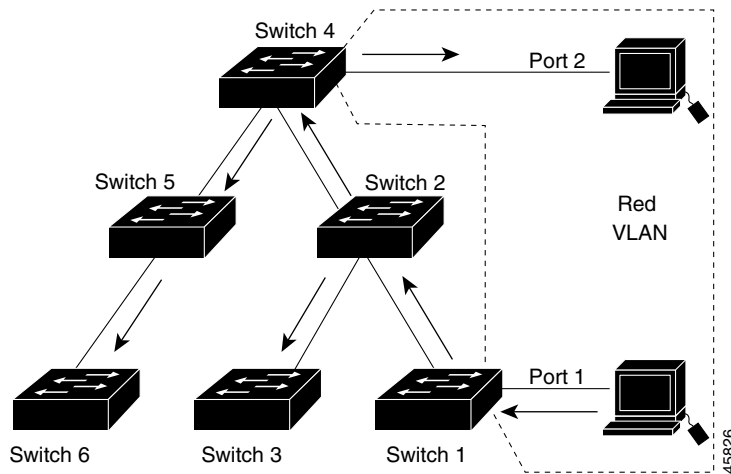
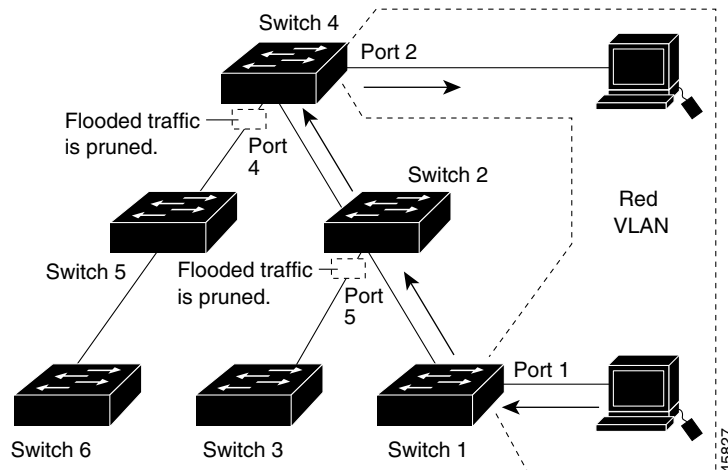
**Figure 9-2 Flooding Traffic without VTP Pruning**

Figure 9-3 shows a switched network with VTP pruning enabled. The broadcast traffic from Switch 1 is not forwarded to Switches 3, 5, and 6 because traffic for the Red VLAN has been pruned on the links shown (Port 5 on Switch 2 and Port 4 on Switch 4).

**Figure 9-3 Optimized Flooded Traffic with VTP Pruning**

Enabling VTP pruning on a VTP server enables pruning for the entire management domain. See the “[Enabling VTP Pruning](#)” section on page 9-13. VTP pruning takes effect several seconds after you enable it. VTP pruning does not prune traffic from VLANs that are pruning-eligible. VLAN 1 is always pruning-eligible; traffic from VLAN 1 cannot be pruned.

VTP pruning is not designed to function in VTP transparent mode. If one or more switches in the network are in VTP transparent mode, you should do one of these:

- Turn off VTP pruning in the entire network.
- Turn off VTP pruning by making all VLANs on the trunk of the switch upstream to the VTP transparent switch pruning ineligible.

To configure VTP pruning on an interface, use the **switchport trunk pruning vlan** interface configuration command (see the “[Changing the Pruning-Eligible List](#)” section on page 9-28). VTP pruning operates when an interface is trunking. You can set VLAN pruning-eligibility, whether or not VTP pruning is enabled for the VTP domain, whether or not any given VLAN exists, and whether or not the interface is currently trunking.

## Configuring VTP

This section includes procedures for configuring VTP. These sections are included:

- [Default VTP Configuration](#), page 9-8
- [VTP Configuration Guidelines](#), page 9-8
- [Configuring a VTP Server](#), page 9-10
- [Configuring a VTP Client](#), page 9-11
- [Disabling VTP \(VTP Transparent Mode\)](#), page 9-11
- [Enabling VTP Version 2](#), page 9-12
- [Enabling VTP Pruning](#), page 9-13
- [Monitoring VTP](#), page 9-13

### Default VTP Configuration

Table 9-3 shows the default VTP configuration.

**Table 9-3** Default VTP Configuration

| Feature                    | Default Setting        |
|----------------------------|------------------------|
| VTP domain name            | Null.                  |
| VTP mode                   | Server.                |
| VTP version 2 enable state | Version 2 is disabled. |
| VTP password               | None.                  |
| VTP pruning                | Disabled.              |

### VTP Configuration Guidelines

These sections describe guidelines you should follow when implementing VTP in your network.

#### Domain Names

When configuring VTP for the first time, you must always assign a domain name. You must configure all switches in the VTP domain with the same domain name. Switches in VTP transparent mode do not exchange VTP messages with other switches, and you do not need to configure a VTP domain name for them.



**Note**

If NVRAM and DRAM storage is sufficient, all switches in a VTP domain should be in VTP server mode.

## Passwords

You can configure a password for the VTP domain, but it is not required. If you do configure a domain password, all domain switches must share the same password and you must configure the password on each switch in the management domain. Switches without a password or with the wrong password reject VTP advertisements.

If you configure a VTP password for a domain, a switch that is booted without a VTP configuration does not accept VTP advertisements until you configure it with the correct password. After the configuration, the switch accepts the next VTP advertisement that uses the same password and domain name in the advertisement.

If you are adding a new switch to an existing network with VTP capability, the new switch learns the domain name only after the applicable password has been configured on it.



### Caution

---

When you configure a VTP domain password, the management domain does not function properly if you do not assign a management domain password to each switch in the domain.

---

## VTP Version

Follow these guidelines when deciding which VTP version to implement:

- All switches in a VTP domain must run the same VTP version.
- A VTP version 2-capable switch can operate in the same VTP domain as a switch running VTP version 1 if version 2 is disabled on the version 2-capable switch (version 2 is disabled by default).
- Do not enable VTP version 2 on a switch unless all of the switches in the same VTP domain are version-2-capable. When you enable version 2 on a switch, all of the version-2-capable switches in the domain enable version 2. If there is a version 1-only switch, it does not exchange VTP information with switches with version 2 enabled.
- If there are TrBRF and TrCRF Token Ring networks in your environment, you must enable VTP version 2 for Token Ring VLAN switching to function properly. To run Token Ring and Token Ring-Net, disable VTP version 2.
- Enabling or disabling VTP pruning on a VTP server enables or disables VTP pruning for the entire VTP domain.
- Making VLANs pruning-eligible or pruning-ineligible affects pruning eligibility for those VLANs on that device only (not on all switches in the VTP domain.)

## Configuration Requirements

When you configure VTP, you must configure a trunk port so that the switch can send and receive VTP advertisements. For more information, see the [“Understanding VLAN Trunks” section on page 9-22](#).

You can configure VTP by entering commands in the VLAN configuration mode. When you enter the **exit** command in VLAN configuration mode, it applies all the commands that you entered. VTP messages are sent to other switches in the VTP domain, and the privileged EXEC mode prompt appears.



### Note

---

The Cisco IOS **end** and **Ctrl-Z** commands are not supported in VLAN configuration mode.

---

For more configuration guidelines, see the [“VLAN Configuration Guidelines” section on page 9-16](#).

## Configuring a VTP Server

When a switch is in VTP server mode, you can change the VLAN configuration and have it propagated throughout the network.

Beginning in privileged EXEC mode, follow these steps to configure the switch as a VTP server:

|        | Command                                   | Purpose   |
|--------|---|---|
| Step 1 | <b>vlan database</b>                      | Enter VLAN configuration mode.  |
| Step 2 | <b>vtp server</b>                         | Configure the switch for VTP server mode (the default).   |
| Step 3 | <b>vtp domain</b> <i>domain-name</i>      | Configure a VTP administrative-domain name.<br><br>The name can be from 1 to 32 characters.<br><br>All switches operating in VTP server or client mode under the same administrative responsibility must be configured with the same domain name. |
| Step 4 | <b>vtp password</b> <i>password-value</i> | (Optional) Set a password for the VTP domain. The password can be from 8 to 64 characters.<br><br>If you configure a VTP password, the VTP domain does not function properly if you do not assign the same password to each switch in the domain. |
| Step 5 | <b>exit</b>                               | Update the VLAN database, propagate it throughout the administrative domain, and return to privileged EXEC mode.  |
| Step 6 | <b>show vtp status</b>                    | Verify your entries in the <i>VTP Operating Mode</i> and the <i>VTP Domain Name</i> fields of the display.  |

When you configure a domain name, it cannot be removed; you can only reassign a switch to a different domain.

To return the switch to a no-password state, use the **no vtp password** VLAN configuration command.

This example shows how to configure the switch as a VTP server with the domain name *eng\_group* and verify the configuration:

```
Switch# vlan database
Switch(vlan)# vtp domain eng_group
Switch(vlan)# exit
APPLY completed.
Exiting...
Switch# show vtp status
VTP Version                : 2
Configuration Revision     : 211
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 8
VTP Operating Mode         : Server
VTP Domain Name            : eng_group
VTP Pruning Mode           : Disabled
VTP V2 Mode                : Disabled
VTP Traps Generation       : Disabled
MD5 digest                 : 0x31 0xB3 0xCD 0xEF 0x34 0xD2 0x44 0xAD
Configuration last modified by 172.20.135.204 at 3-1-93 00:05:51
Local updater ID is 172.20.135.202 on interface V11 (lowest numbered VLAN interface found)
```

## Configuring a VTP Client

When a switch is in VTP client mode, you cannot change its VLAN configuration. The client switch receives VTP updates from a VTP server in the VTP domain and then modifies its configuration accordingly.

Beginning in privileged EXEC mode, follow these steps to configure the switch for VTP client mode:

|        | Command                                   | Purpose   |
|--------|---|---|
| Step 1 | <b>vlan database</b>                      | Enter VLAN configuration mode.  |
| Step 2 | <b>vtp client</b>                         | Configure the switch for VTP client mode. The default setting is VTP server.  |
| Step 3 | <b>vtp domain</b> <i>domain-name</i>      | Configure a VTP administrative-domain name. The name can be from 1 to 32 characters. This should be the same domain name as the VTP server.<br><br>All switches operating in VTP server or client mode under the same administrative responsibility must be configured with the same domain name. |
| Step 4 | <b>vtp password</b> <i>password-value</i> | (Optional) Assign a password for the VTP domain. The password can be from 8 to 64 characters.<br><br>If you configure a VTP password, the VTP domain does not function properly if you do not assign the same password to each switch in the domain.  |
| Step 5 | <b>exit</b>                               | Update the VLAN database, propagate it throughout the administrative domain, and return to privileged EXEC mode.  |
| Step 6 | <b>show vtp status</b>                    | Verify your entries in the <i>VTP Operating Mode</i> field of the display.  |

Use the **no vtp client** VLAN configuration command to return the switch to VTP server mode. To return the switch to a no-password state, use the **no vtp password** VLAN configuration command. When you configure a domain name, it cannot be removed; you can only reassign a switch to a different domain.

## Disabling VTP (VTP Transparent Mode)

When you configure the switch for VTP transparent mode, you disable VTP on the switch. The switch then does not send VTP updates and does not act on VTP updates received from other switches. However, a VTP transparent switch running VTP version 2 does forward received VTP advertisements on all of its trunk links.

Beginning in privileged EXEC mode, follow these steps to configure the switch for VTP transparent mode:

|        | Command                | Purpose   |
|--------|------------------------|---|
| Step 1 | <b>vlan database</b>   | Enter VLAN configuration mode.  |
| Step 2 | <b>vtp transparent</b> | Configure the switch for VTP transparent mode.<br><br>The default setting is VTP server.<br><br>This step disables VTP on the switch. |

|        | Command         | Purpose  |
|--------|-----------------|--|
| Step 3 | exit            | Update the VLAN database, propagate it throughout the administrative domain, and return to privileged EXEC mode. |
| Step 4 | show vtp status | Verify your entries in the <i>VTP Operating Mode</i> field of the display.                                       |

To return the switch to VTP server mode, use the **no vtp transparent** VLAN configuration command.

## Enabling VTP Version 2

VTP version 2 is disabled by default on VTP version 2-capable switches. When you enable VTP version 2 on a switch, every VTP version 2-capable switch in the VTP domain enables version 2.



### Caution

VTP version 1 and VTP version 2 are not interoperable on switches in the same VTP domain. Every switch in the VTP domain must use the same VTP version. Do not enable VTP version 2 unless every switch in the VTP domain supports version 2.



### Note

In TrCRF and TrBRF Token ring environments, you must enable VTP version 2 for Token Ring VLAN switching to function properly. For Token Ring and Token Ring-Net media, VTP version 2 must be disabled.

For more information on VTP version configuration guidelines, see the [“VTP Version” section on page 9-9](#).

Beginning in privileged EXEC mode, follow these steps to enable VTP version 2:

|        | Command         | Purpose  |
|--------|-----------------|--|
| Step 1 | vlan database   | Enter VLAN configuration mode.   |
| Step 2 | vtp v2-mode     | Enable VTP version 2 on the switch.<br>VTP version 2 is disabled by default on VTP version 2-capable switches.   |
| Step 3 | exit            | Update the VLAN database, propagate it throughout the administrative domain, and return to privileged EXEC mode. |
| Step 4 | show vtp status | Verify that VTP version 2 is enabled in the <i>VTP V2 Mode</i> field of the display.                             |

To disable VTP version 2, use the **no vtp v2-mode** VLAN configuration command.

## Enabling VTP Pruning

Pruning increases available bandwidth by restricting flooded traffic to those trunk links that the traffic must use to access the destination devices. You enable VTP pruning on a switch in VTP server mode.

Beginning in privileged EXEC mode, follow these steps to enable VTP pruning in the management domain:

|        | Command                | Purpose  |
|--------|------------------------|--|
| Step 1 | <b>vlan database</b>   | Enter VLAN configuration mode.   |
| Step 2 | <b>vtp pruning</b>     | Enable pruning in the VTP administrative domain.<br>By default, pruning is disabled. You need to enable pruning on only one switch in VTP server mode. |
| Step 3 | <b>exit</b>            | Update the VLAN database, propagate it throughout the administrative domain, and return to privileged EXEC mode.                                       |
| Step 4 | <b>show vtp status</b> | Verify your entries in the <i>VTP Pruning Mode</i> field of the display.   |

Pruning is supported with VTP version 1 and version 2. If you enable pruning on the VTP server, it is enabled for the entire VTP domain.

Only VLANs included in the pruning-eligible list can be pruned. By default, VLANs 2 through 1001 are pruning eligible on trunk ports. To change the pruning-eligible VLANs, see the [“Changing the Pruning-Eligible List” section on page 9-28](#).

To disable VTP pruning, use the **no vtp pruning** VLAN configuration command.

## Monitoring VTP

You monitor VTP by displaying VTP configuration information: the domain name, the current VTP revision, and the number of VLANs. You can also display statistics about the advertisements sent and received by the switch.

Beginning in privileged EXEC mode, follow these steps to monitor VTP activity:

**Table 9-4 VTP Monitoring Commands**

| Command                  | Purpose   |
|--------------------------|---|
| <b>show vtp status</b>   | Display the VTP switch configuration information.                     |
| <b>show vtp counters</b> | Display counters about VTP messages that have been sent and received. |

This is an example of output from the **show vtp status** privileged EXEC command:

```
Switch# show vtp status
VTP Version                : 2
Configuration Revision     : 5
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 69
VTP Operating Mode         : Server
VTP Domain Name            : test
VTP Pruning Mode           : Disabled
VTP V2 Mode                : Disabled
VTP Traps Generation       : Disabled
MD5 digest                 : 0x59 0xBA 0x92 0xA4 0x74 0xD5 0x42 0x29
Configuration last modified by 0.0.0.0 at 3-1-93 00:18:42
Local updater ID is 10.1.1.59 on interface Vl1 (lowest numbered VLAN interface found)
```

This is an example of output from the **show vtp counters** privileged EXEC command:

```
Switch# show vtp counters
VTP statistics:
Summary advertisements received      : 0
Subset advertisements received      : 0
Request advertisements received     : 0
Summary advertisements transmitted  : 0
Subset advertisements transmitted   : 0
Request advertisements transmitted  : 0
Number of config revision errors    : 0
Number of config digest errors      : 0
Number of V1 summary errors         : 0

VTP pruning statistics:

Trunk          Join Transmitted Join Received      Summary advts received from
-----          -----          -----          -----
non-pruning-capable device
```

# VLANs in the VTP Database

You can set these parameters when you create a new VLAN or modify an existing VLAN in the VTP 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)
- 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

The “[Default VLAN Configuration](#)” section on page 9-15 lists the default values and possible ranges for each VLAN media type.

## Token Ring VLANs

Although the Catalyst 3550 switches do not support Token Ring connections, a remote device such as a Catalyst 5000 series switch with Token Ring connections could be managed from one of the supported switches. Switches running VTP version 2 advertise information about these Token Ring VLANs:

- Token Ring TrBRF VLANs
- Token Ring TrCRF VLANs

For more information on configuring Token Ring VLANs, see the *Catalyst 5000 Series Software Configuration Guide*.

## Default VLAN Configuration

[Table 9-5](#) shows the default configuration for Ethernet VLANs.

**Note**

---

The switch supports Ethernet interfaces exclusively. Because FDDI and Token Ring VLANs are not locally supported, you only configure FDDI and Token Ring media-specific characteristics for VTP global advertisements to other switches.

---

**Table 9-5 Ethernet VLAN Defaults and Ranges**

| Parameter              | Default | Range           |
|------------------------|---------|-----------------|
| VLAN ID                | 1       | 1–1005          |
| VLAN name              | default | No range        |
| 802.10 SAID            | 101001  | 1–4294967294    |
| MTU size               | 1500    | 1500–18190      |
| Translational bridge 1 | 1002    | 0–1005          |
| Translational bridge 2 | 1003    | 0–1005          |
| VLAN state             | active  | active, suspend |

## VLAN Configuration Guidelines

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

- The Catalyst 3550 switch supports 1005 VLANs in VTP client, server, and transparent modes. VLANs are identified with a number between 1 and 1001. VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs.
- Before you can create a VLAN, the switch must be in VTP server mode or VTP transparent mode. If the switch is a VTP server, you must define a VTP domain.
- Catalyst 3550 switches do not support Token Ring or FDDI media. The switch does not forward FDDI, FDDI-Net, TrCRF, or TrBRF traffic, but it does propagate the VLAN configuration through VTP.
- The switch supports 128 spanning-tree instances. If a switch has more active VLANs than supported spanning-tree instances, STP 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 anywhere in the VTP domain 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 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 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.
- A port in dynamic mode can negotiate with its neighbor to become a trunk port. If you try to enable 802.1X on a dynamic 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 dynamic, the port mode is not changed.

## Configuring VLANs in the VTP Database

You can add, modify or remove VLAN configurations in the VTP database by using the CLI VLAN configuration mode. VTP globally propagates these VLAN changes throughout the VTP domain.

In VTP server or transparent mode, commands to add, change, and delete VLANs are written to the file `vlan.dat`, and you can display them by entering the **show vlan** privileged EXEC command. The `vlan.dat` file is stored in NVRAM.



### Caution

You can cause inconsistency in the VLAN database if you attempt to manually delete the `vlan.dat` file. If you want to modify the VLAN configuration or VTP, use the **vlan database** privileged EXEC command to enter VLAN configuration mode as described in the *Catalyst 3550 Multilayer Switch Command Reference* for this release.

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.



### Note

VLANs can be configured to support a number of parameters that are not discussed in detail in this section. For complete information on the commands and parameters that control VLAN configuration, refer to the *Catalyst 3550 Multilayer Switch Command Reference* for this release.

## Adding an Ethernet VLAN

Each Ethernet VLAN has a unique, 4-digit ID that can be a number from 1 to 1001. To add a VLAN to the VLAN database, assign a number and name to the VLAN. For the list of default parameters that are assigned when you add a VLAN, see the “[Default VLAN Configuration](#)” section on page 9-15.

Beginning in privileged EXEC mode, follow these steps to add an Ethernet VLAN:

|        | Command  | Purpose  |
|--------|--|--|
| Step 1 | <b>vlan database</b>   | Enter VLAN configuration mode.   |
| Step 2 | <b>vlan</b> <i>vlan-id</i> <b>name</b> <i>vlan-name</i>          | Add an Ethernet VLAN by assigning a number to it. If no name is entered for the VLAN, the default is to append the <i>vlan-id</i> to the word VLAN. For example, VLAN0004 could be a default VLAN name for VLAN 4. |
| Step 3 | <b>exit</b>  | Update the VLAN database, propagate it throughout the administrative domain, and return to privileged EXEC mode.   |
| Step 4 | <b>show vlan name</b> <i>vlan-name</i><br>or<br><b>show vlan</b> | Verify your entries.   |

To return the VLAN name to the default setting, use the **no vlan** *vlan-id* **name** VLAN configuration command.

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

```
Switch# vlan database
Switch(vlan)# vlan 20 name test20
Switch(vlan)# exit
APPLY completed.
Exiting...
Switch# show vlan name test20
```

| VLAN Name | Status | Ports |
|-----------|--------|-------|
| 20 test20 | active |       |

| VLAN | Type | SAID   | MTU  | Parent | RingNo | BridgeNo | Stp | BrdgMode | Trans1 | Trans2 |
|------|------|--------|------|--------|--------|----------|-----|----------|--------|--------|
| 20   | enet | 100020 | 1500 | -      | -      | -        | -   | -        | 0      | 0      |

## Modifying an Ethernet VLAN

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

|        | Command  | Purpose  |
|--------|--|--|
| Step 1 | <b>vlan database</b>   | Enter VLAN configuration mode.   |
| Step 2 | <b>vlan <i>vlan-id</i> mtu <i>mtu-size</i></b>               | Identify the VLAN, and change the MTU size.  |
| Step 3 | <b>exit</b>  | Update the VLAN database, propagate it throughout the administrative domain, and return to privileged EXEC mode. |
| Step 4 | <b>show vlan id <i>vlan-id</i></b><br>or<br><b>show vlan</b> | Verify your entries.   |

To return the VLAN to the default MTU setting, use the **no vlan *vlan-id* mtu** VLAN configuration command.

This example shows how to verify a VLAN configuration:

```
Switch# show vlan id 20
```

| VLAN Name      | Status | Ports |
|----------------|--------|-------|
| show vlan----- |        |       |
| 20 VLAN0020    | active |       |

| VLAN | Type | SAID   | MTU  | Parent | RingNo | BridgeNo | Stp | BrdgMode | Trans1 | Trans2 |
|------|------|--------|------|--------|--------|----------|-----|----------|--------|--------|
| 20   | enet | 100020 | 1500 | -      | -      | -        | -   | -        | 0      | 0      |

## Deleting a VLAN from the Database

When you delete a VLAN from a switch that is in VTP server mode, the VLAN is removed from all switches in the VTP domain. When you delete a VLAN from a switch that is in VTP transparent mode, the VLAN is deleted only on that specific switch.

You cannot delete the default VLANs for the different media types: Ethernet VLAN 1 and FDDI or Token Ring 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.

Beginning in privileged EXEC mode, follow these steps to delete a VLAN on the switch:

|        | Command                       | Purpose  |
|--------|-------------------------------|--|
| Step 1 | <b>vlan database</b>          | Enter VLAN configuration mode.   |
| Step 2 | <b>no vlan <i>vlan-id</i></b> | Remove the VLAN by entering the VLAN ID.   |
| Step 3 | <b>exit</b>                   | Update the VLAN database, propagate it throughout the administrative domain, and return to privileged EXEC mode. |
| Step 4 | <b>show vlan brief</b>        | Verify the VLAN removal.   |

This example shows how to verify a VLAN removal by using the **show vlan brief** privileged EXEC command:

```
Switch# show vlan brief
```

```

VLAN Name                Status    Ports
-----
1    default                 active   Gi0/1, Gi0/2, Gi0/3, Gi0/4
                                     Gi0/5, Gi0/7, Gi0/8, Gi0/9
                                     Gi0/10, Gi0/11, Gi0/12
11   VLAN0011                active
20   VLAN0020                active
129  VLAN0129                active
1002 fddi-default            active
1003 token-ring-default    active
1004 fddinet-default        active
1005 trnet-default         active

```

## Assigning Static-Access Ports to a VLAN

You can assign a static-access port to a VLAN without having VTP globally propagate VLAN configuration information (VTP is disabled).

**Note**

If you assign an interface to a VLAN that does not exist, the new VLAN is created. (See the [“Adding an Ethernet VLAN”](#) section on page 9-17.)

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

|        | Command                                      | Purpose   |
|--------|--|---|
| Step 1 | <b>configure terminal</b>                    | Enter global configuration mode                                     |
| Step 2 | <b>interface <i>interface-id</i></b>         | Enter the interface to be added to the VLAN.                        |
| Step 3 | <b>switchport mode access</b>                | Define the VLAN membership mode for the port (Layer 2 access port). |
| Step 4 | <b>switchport access vlan <i>vlan-id</i></b> | Assign the port to a VLAN.  |
| Step 5 | <b>end</b>                                   | Return to privileged EXEC mode.                                     |

|        | Command  | Purpose  |
|--------|--|--|
| Step 6 | <b>show running-config interface</b> <i>interface-id</i>     | Verify the VLAN membership mode of the interface.  |
| Step 7 | <b>show interfaces</b> <i>interface-id</i> <b>switchport</b> | Verify your entries in the <i>Administrative Mode</i> and the <i>Access Mode VLAN</i> fields of the display. |
| Step 8 | <b>copy running-config startup-config</b>                    | (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 Gigabit Ethernet interface 0/1 as an access port in VLAN 2:

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

These examples show how to verify the configuration:

```
Switch# show running-config interface gigabitethernet0/1
Building configuration...
```

```
Current configuration : 74 bytes
!
interface GigabitEthernet0/1
  no ip address
  snmp trap link-status
end
```

```
Switch# show interfaces gigabitethernet0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
```

```
Protected: false
Unknown unicast blocked: false
Unknown multicast blocked: false
```

```
Broadcast Suppression Level: 100
Multicast Suppression Level: 100
Unicast Suppression Level: 100
```

## Displaying VLANs in the VTP Database

Use the **show vlan** privileged EXEC command to display a list of VLANs in the database, including status, ports, and configuration:

```
Switch# show vlan
```

```

VLAN Name                Status    Ports
-----
1    default                active    Gi0/1, Gi0/2, Gi0/3, Gi0/4
                                           Gi0/7, Gi0/8, Gi0/9, Gi0/11
                                           Gi0/12

20   VLAN0020              active
21   VLAN0021              active
22   VLAN0022              active
27   VLAN0027              active
31   VLAN0031              active
1002 fddi-default          active
1003 trcrf-default        active
1004 fddinet-default      active
1005 trbrf-default        active

VLAN Type  SAID      MTU    Parent RingNo BridgeNo  Stp  BrdgMode Trans1 Trans2
-----
1    enet  100001   1500   -      -      -      -    -      1002  1003
20   enet  100020   1500   -      -      -      -    -      0      0
21   enet  100021   1500   -      -      -      -    -      0      0

VLAN Type  SAID      MTU    Parent RingNo BridgeNo  Stp  BrdgMode Trans1 Trans2
-----
22   enet  100022   1500   -      -      -      -    -      0      0
27   enet  100027   1500   -      -      -      -    -      0      0
31   enet  100031   1500   -      -      -      -    -      0      0
1002 fddi  101002   1500   -      -      -      -    -      1      1003
1003 trcrf 101003   4472   1005   3276   -      -    srb    1      1002
1004 fdnet 101004   1500   -      -      1      -    ibm    -      0
1005 trbrf 101005   4472   -      -      15     -    ibm    -      0

VLAN AREHops STEHops Backup CRF
-----
1003 7          7          off

```

Use the **show vlan brief** privileged EXEC command to display a list of VLANs in the database with status and port information but without configuration information:

```
Switch# show vlan brief
```

```

VLAN Name                Status    Ports
-----
1    default                active    Gi0/1, Gi0/2, Gi0/3, Gi0/4
                                           Gi0/7, Gi0/8, Gi0/9, Gi0/11
                                           Gi0/12

20   VLAN0020              active
21   VLAN0021              active
22   VLAN0022              active
27   VLAN0027              active
31   VLAN0031              active
1002 fddi-default          active
1003 trcrf-default        active
1004 fddinet-default      active
1005 trbrf-default        active

```

# Understanding VLAN Trunks

These sections describe how VLAN trunks function on the switch:

- [Trunking Overview, page 9-22](#)
- [Encapsulation Types, page 9-23](#)
- [Default Layer 2 Ethernet Interface VLAN Configuration, page 9-24](#)

## Trunking Overview

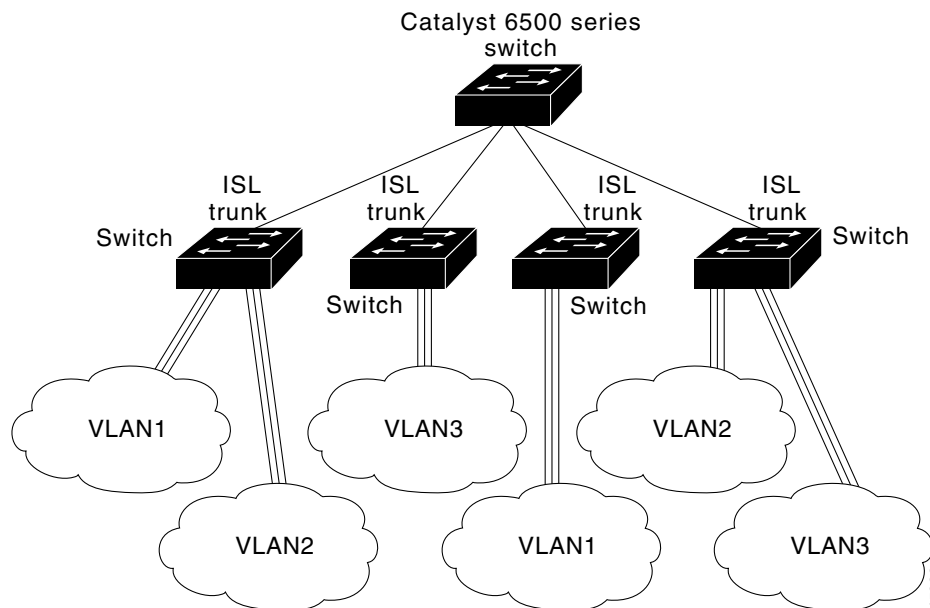
A trunk is a point-to-point link between one or more Ethernet switch interfaces and another networking device such as a router or a switch. Trunks carry the traffic of multiple VLANs over a single link, and you can extend VLANs across an entire network. The 100BASE-T and Gigabit Ethernet trunks carry traffic for multiple VLANs over a single link.

Two trunking encapsulations are available on all Ethernet interfaces:

- Inter-Switch Link (ISL)—ISL is Cisco-proprietary trunking encapsulation.
- 802.1Q—802.1Q is industry-standard trunking encapsulation.

Figure 9-4 shows a network of switches that are connected by ISL trunks.

**Figure 9-4** Switches in an ISL Trunking Environment



You can configure a trunk on a single Ethernet interface or on an EtherChannel bundle. For more information about EtherChannel, see [Chapter 21, “Configuring EtherChannel.”](#)

Ethernet trunk interfaces support different trunking modes (see [Table 9-6](#)). You can specify whether the trunk uses ISL or 802.1Q encapsulation or if the encapsulation type is autonegotiated. To autonegotiate trunking, the interfaces must be in the same VTP domain. Use the **trunk** or **nonegotiate** keywords to force interfaces in different domains to trunk. Trunk negotiation is managed by the Dynamic Trunking Protocol (DTP), which supports autonegotiation of both ISL and 802.1Q trunks.

**Note**

DTP is a point-to-point protocol. However, some internetworking devices might forward DTP frames improperly. To avoid this, ensure that interfaces connected to devices that do not support DTP are configured with the **access** keyword if you do not intend to trunk across those links. To enable trunking to a device that does not support DTP, use the **nonegotiate** keyword to cause the interface to become a trunk but to not generate DTP frames.

**Table 9-6 Layer 2 Interface Modes**

| Mode                                     | Function   |
|--|--|
| <b>switchport mode access</b>            | 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 even if the neighboring interface is not a trunk interface.   |
| <b>switchport mode dynamic desirable</b> | Makes the interface actively attempt to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to <i>trunk</i> , <i>desirable</i> , or <i>auto</i> mode. The default switch-port mode for all Ethernet interfaces is <b>dynamic desirable</b> . |
| <b>switchport mode dynamic auto</b>      | Makes the interface able to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to <i>trunk</i> or <i>desirable</i> mode.  |
| <b>switchport mode trunk</b>             | Puts the interface into permanent trunking mode and negotiates to convert the link into a trunk link. The interface becomes a trunk interface even if the neighboring interface is not a trunk interface.  |
| <b>switchport nonegotiate</b>            | Puts the interface into permanent trunking mode but prevents the interface from generating DTP frames. You must manually configure the neighboring interface as a trunk interface to establish a trunk link.   |

## Encapsulation Types

Table 9-7 lists the Ethernet trunk encapsulation types and keywords.

**Table 9-7 Ethernet Trunk Encapsulation Types**

| Encapsulation                                   | Function  |
|---|---|
| <b>switchport trunk encapsulation isl</b>       | Specifies ISL encapsulation on the trunk link.  |
| <b>switchport trunk encapsulation dot1q</b>     | Specifies 802.1Q encapsulation on the trunk link.   |
| <b>switchport trunk encapsulation negotiate</b> | Specifies that the interface negotiate with the neighboring interface to become an ISL (preferred) or 802.1Q trunk, depending on the configuration and capabilities of the neighboring interface. |

**Note**

The switch does not support Layer 3 trunks; you cannot configure subinterfaces or use the **encapsulation** keyword on Layer 3 interfaces. The switch does support Layer 2 trunks and Layer 3 VLAN interfaces, which provide equivalent capabilities.

The trunking mode, the trunk encapsulation type, and the hardware capabilities of the two connected interfaces determine whether a link becomes an ISL or 802.1Q trunk.

## 802.1Q Configuration Considerations

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

## Default Layer 2 Ethernet Interface VLAN Configuration

Table 9-8 shows the default Layer 2 Ethernet interface VLAN configuration.

**Table 9-8** Default Layer 2 Ethernet Interface VLAN Configuration

| Feature                         | Default Setting                                 |
|---------------------------------|---|
| Interface mode                  | <b>switchport mode dynamic desirable</b>        |
| Trunk encapsulation             | <b>switchport trunk encapsulation negotiate</b> |
| Allowed VLAN range              | VLANs 1–1005                                    |
| VLAN range eligible for pruning | VLANs 2–1001                                    |
| Default VLAN (for access ports) | VLAN 1  |
| Native VLAN (for 802.1Q trunks) | VLAN 1  |

## Configuring an Ethernet Interface as a Trunk Port

Because trunk ports send and receive VTP advertisements, you must ensure that at least one trunk port is configured on the switch and that this trunk port is connected to the trunk port of a second switch. Otherwise, the switch cannot receive any VTP advertisements.

This section includes these procedures for configuring an Ethernet interface as a trunk port on the switch:

- [Configuring a Trunk Port, page 9-25](#)
- [Defining the Allowed VLANs on a Trunk, page 9-27](#)
- [Changing the Pruning-Eligible List, page 9-28](#)
- [Configuring the Native VLAN for Untagged Traffic, page 9-29](#)



### Note

By default, an interface is in Layer 2 mode. The default mode for Layer 2 interfaces is **switchport mode dynamic desirable**. If the neighboring interface supports trunking and is configured to allow trunking, the link is a Layer 2 trunk or, if the interface is in Layer 3 mode, it becomes a Layer 2 trunk when you enter the **switchport** interface configuration command. By default, trunks negotiate encapsulation. If the neighboring interface supports ISL and 802.1Q encapsulation and both interfaces are set to negotiate the encapsulation type, the trunk uses ISL encapsulation.

## Configuring a Trunk Port

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

|        | Command   | Purpose   |
|--------|---|---|
| Step 1 | <b>configure terminal</b>                                       | Enter global configuration mode.  |
| Step 2 | <b>interface</b> <i>interface-id</i>                            | Enter the interface configuration mode and the port to be configured for trunking.  |
| Step 3 | <b>switchport trunk encapsulation</b> {isl   dot1q   negotiate} | Configure the port to support ISL or 802.1Q encapsulation or to negotiate (the default) with the neighboring interface for encapsulation type.<br>You must configure each end of the link with the same encapsulation type.   |
| Step 4 | <b>switchport mode</b> {dynamic {auto   desirable}   trunk}     | 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). <ul style="list-style-type: none"> <li>• <b>dynamic auto</b>—Set the interface to a trunk link if the neighboring interface is set to trunk or desirable mode.</li> <li>• <b>dynamic desirable</b>—Set the interface to a trunk link if the neighboring interface is set to trunk, desirable, or auto mode.</li> <li>• <b>trunk</b>—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.</li> </ul> |
| Step 5 | <b>switchport access vlan</b> <i>vlan-id</i>                    | (Optional) Specify the default VLAN, which is used if the interface stops trunking.   |
| Step 6 | <b>switchport trunk native vlan</b> <i>vlan-id</i>              | For 802.1Q trunks, specify the native VLAN.   |
| Step 7 | <b>end</b>  | Return to privileged EXEC mode.   |

|         | Command  | Purpose   |
|---------|--|---|
| Step 8  | <b>show interfaces interface-id switchport</b> | Display the switchport configuration of the interface in the <i>Administrative Mode</i> and the <i>Administrative Trunking Encapsulation</i> fields of the display. |
| Step 9  | <b>show interfaces interface-id trunk</b>      | Display the trunk configuration of the interface.   |
| Step 10 | <b>copy running-config startup-config</b>      | (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. Use the **no switchport mode** and **no switchport access** interface configuration commands to return to the default settings.

This example shows how to configure the Gigabit Ethernet interface 0/4 as an 802.1Q trunk. This example assumes that the neighbor interface is configured to support 802.1Q trunking:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/4
Switch(config-if)# switchport mode dynamic desirable
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# end
Switch#
```

These examples show how to verify the configuration:

```
Switch# show running-config interface gigabitethernet0/4
Building configuration...

Current configuration : 112 bytes
!
interface GigabitEthernet0/4
 switchport trunk encapsulation dot1q
 no ip address
 snmp trap link-status
end

Switch# show interfaces gigabitethernet0/4 switchport
Name: Gi0/4
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001

Protected: false
Unknown unicast blocked: false
Unknown multicast blocked: false

Broadcast Suppression Level: 100
Multicast Suppression Level: 100
Unicast Suppression Level: 100
```

In this example, the encapsulation method is ISL:

```
Switch# show interfaces gigabitethernet0/4 trunk

Port      Mode           Encapsulation  Status      Native vlan
Gi0/4     desirable     n-isl          trunking    1

Port      Vlans allowed on trunk
Gi0/4     1-1005

Port      Vlans allowed and active in management domain
Gi0/4     1,10-1000

Port      Vlans in spanning tree forwarding state and not pruned
Gi0/4     1,10-1000
```

## Defining the Allowed VLANs on a Trunk

By default, a trunk port sends traffic to and receives traffic from all VLANs in the VLAN database. All VLANs, VLANs 1 to 1005, 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 to remove specific VLANs from the allowed list.

A trunk port can become a member of a VLAN if the VLAN is enabled, if VTP knows of the VLAN, and if the VLAN is in the allowed list for the port. When VTP detects a newly enabled VLAN and the VLAN is in the allowed list for a trunk port, the trunk port automatically becomes a member of the enabled VLAN. When VTP detects a new VLAN and the VLAN is not in the allowed list for a trunk port, the trunk port does not become a member of the new VLAN.

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

|        | Command  | Purpose  |
|--------|--|--|
| Step 1 | <b>configure terminal</b>  | Enter global configuration mode.   |
| Step 2 | <b>interface <i>interface-id</i></b>   | Enter interface configuration mode and the port to be added to the VLAN.   |
| Step 3 | <b>switchport trunk allowed vlan {add   except   none   remove} <i>vlan-list</i></b> | (Optional) Configure the list of VLANs allowed on the trunk.<br>For explanations about using the <b>add</b> , <b>except</b> , <b>none</b> , and <b>remove</b> keywords, refer to <i>Catalyst 3550 Multilayer Switch Command Reference</i> for this release.<br>The <i>vlan-list</i> parameter is either a single VLAN number from 1 to 1005 or a range of VLANs described by two VLAN numbers, the lesser 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. You cannot remove any of the default VLANs from a trunk. |
| Step 4 | <b>end</b>   | Return to privileged EXEC.   |
| Step 5 | <b>show interfaces <i>interface-id</i> switchport</b>                                | Verify your entries in the <i>Trunking VLANs Enabled</i> field of the display.   |
| Step 6 | <b>copy running-config startup-config</b>  | (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 and verify the configuration.

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport trunk allowed vlan remove 2
Switch(config-if)# end
Switch# show interfaces gigabitethernet0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: 1,3-1005
Pruning VLANs Enabled: 2-1001

Protected: false
Unknown unicast blocked: false
Unknown multicast blocked: false

Broadcast Suppression Level: 100
Multicast Suppression Level: 100
Unicast Suppression Level: 100
```

## Changing the Pruning-Eligible List

The pruning-eligible list applies only to trunk ports. Each trunk port has its own eligibility list. VTP pruning must be enabled for this procedure to take effect. The [“Enabling VTP Pruning” section on page 9-13](#) describes how to enable VTP pruning.

Beginning in privileged EXEC mode, follow these steps to remove VLANs from the pruning-eligible list on a trunk port:

|        | Command   | Purpose   |
|--------|---|---|
| Step 1 | <b>configure terminal</b>   | Enter global configuration mode.  |
| Step 2 | <b>interface</b> <i>interface-id</i>  | Enter interface configuration mode, and select the trunk port for which VLANs should be pruned.   |
| Step 3 | <b>switchport trunk pruning vlan</b> { <b>add</b>   <b>except</b>   <b>none</b>   <b>remove</b> } <i>vlan-list</i><br>[, <i>vlan</i> [, <i>vlan</i> [,.,]]] | Configure the list of VLANs allowed to be pruned from the trunk. (See the <a href="#">“VTP Pruning” section on page 9-6</a> ).<br><br>For explanations about using the <b>add</b> , <b>except</b> , <b>none</b> , and <b>remove</b> keywords, refer to <i>Catalyst 3550 Multilayer Switch Command Reference</i> for this release.<br><br>Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs. Valid IDs are from 2 to 1001.<br><br>VLANs that are pruning-ineligible receive flooded traffic.<br><br>The default list of VLANs allowed to be pruned contains all VLANs. |
| Step 4 | <b>end</b>  | Return to privileged EXEC mode.   |

|        | Command   | Purpose   |
|--------|---|---|
| Step 5 | <b>show interfaces <i>interface-id</i> switchport</b> | Verify your entries in the <i>Pruning VLANs Enabled</i> field of the display. |
| Step 6 | <b>copy running-config startup-config</b>             | (Optional) Save your entries in the configuration file.                       |

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

## 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 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 “[Encapsulation Types](#)” section on page 9-23. Beginning in privileged EXEC mode, follow these steps to configure the native VLAN on an 802.1Q trunk:

|        | Command   | Purpose   |
|--------|---|---|
| Step 1 | <b>configure terminal</b>                             | Enter global configuration mode.  |
| Step 2 | <b>interface <i>interface-id</i></b>                  | Enter interface configuration mode, and define the interface that is configured as the 802.1Q trunk.                  |
| Step 3 | <b>switchport trunk native vlan <i>vlan-id</i></b>    | Configure the VLAN that is sending and receiving untagged traffic on the trunk port.<br>Valid IDs are from 1 to 1001. |
| Step 4 | <b>end</b>  | Return to privileged EXEC mode.   |
| Step 5 | <b>show interfaces <i>interface-id</i> switchport</b> | Verify your entries in the <i>Trunking Native Mode VLAN</i> field.  |
| Step 6 | <b>copy running-config startup-config</b>             | (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 outgoing port native VLAN ID, the packet is sent untagged; otherwise, the switch sends the packet with a tag.

## Load Sharing Using STP

Load sharing divides the bandwidth supplied by parallel trunks connecting 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 which VLAN the traffic belongs.

You configure load sharing on trunk ports 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, see [Chapter 10, “Configuring STP.”](#)

## Load Sharing Using STP Port Priorities

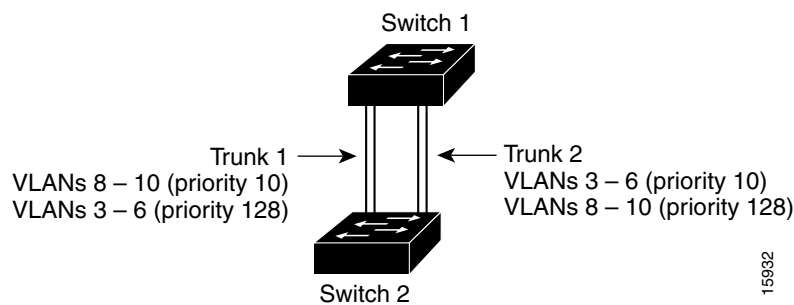
When two ports on the same switch form a loop, the STP port priority setting determines which port is enabled and which port is in a blocking state. You can set the priorities on a parallel trunk port so that the port carries all the traffic for a given VLAN. The trunk port with the higher priority (lower 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 9-5 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 10 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 10 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 9-5 Load Sharing by Using STP Port Priorities**



## Configuring STP Port Priorities and Load Sharing

Beginning in privileged EXEC mode, follow these steps to configure the network shown in Figure 9-5:

|        | Command                             | Purpose   |
|--------|-------------------------------------|---|
| Step 1 | <code>vlan database</code>          | On Switch 1, enter VLAN configuration mode.   |
| Step 2 | <code>vtp domain domain-name</code> | Configure a VTP administrative domain.<br>The domain name can be from 1 to 32 characters.   |
| Step 3 | <code>vtp server</code>             | Configure Switch 1 as the VTP server.   |
| Step 4 | <code>exit</code>                   | Update the VLAN database, propagate it throughout the administrative domain, and return to privileged EXEC mode.  |
| Step 5 | <code>show vtp status</code>        | Verify the VTP configuration on both Switch 1 and Switch 2.<br>In the display, check the <i>VTP Operating Mode</i> and the <i>VTP Domain Name</i> fields. |

|         | <b>Command</b>  | <b>Purpose</b>   |
|---------|---|--|
| Step 6  | <code>show vlan</code>  | Verify that the VLANs exist in the database on Switch 1.   |
| Step 7  | <code>configure terminal</code>                                       | Enter global configuration mode.   |
| Step 8  | <code>interface gigabitethernet 0/1</code>                            | Enter interface configuration mode, and define Gigabit Ethernet port 0/1 as the interface to be configured as a trunk.   |
| Step 9  | <code>switchport trunk encapsulation {isl   dot1q   negotiate}</code> | Configure the port to support ISL or 802.1Q encapsulation or to negotiate with the neighboring interface.<br><br>You must configure each end of the link with the same encapsulation type. |
| Step 10 | <code>switchport mode trunk</code>                                    | Configure the port as a trunk port.  |
| Step 11 | <code>end</code>  | Return to privilege EXEC mode.   |
| Step 12 | <code>show interfaces gigabitethernet0/1 switchport</code>            | Verify the VLAN configuration.   |
| Step 13 |   | Repeat Steps 7 through 11 on Switch 1 for interface Gi0/2.   |
| Step 14 |   | Repeat Steps 7 through 11 on Switch 2 to configure the trunk ports on interface Gi0/1 and Gi0/2.   |
| Step 15 | <code>show vlan</code>  | When the trunk links come up, VTP passes the VTP and VLAN information to Switch 2. Verify that Switch 2 has learned the VLAN configuration.  |
| Step 16 | <code>configure terminal</code>                                       | Enter global configuration mode on Switch 1.   |
| Step 17 | <code>interface gigabitethernet0/1</code>                             | Enter interface configuration mode, and define the interface to set the STP port priority.   |
| Step 18 | <code>spanning-tree vlan 8 port-priority 10</code>                    | Assign the port priority of 10 for VLAN 8.   |
| Step 19 | <code>spanning-tree vlan 9 port-priority 10</code>                    | Assign the port priority of 10 for VLAN 9.   |
| Step 20 | <code>spanning-tree vlan 10 port-priority 10</code>                   | Assign the port priority of 10 for VLAN 10.  |
| Step 21 | <code>exit</code>   | Return to global configuration mode.   |
| Step 22 | <code>interface gigabitethernet0/2</code>                             | Enter interface configuration mode, and define the interface to set the STP port priority.   |
| Step 23 | <code>spanning-tree vlan 3 port-priority 10</code>                    | Assign the port priority of 10 for VLAN 3.   |
| Step 24 | <code>spanning-tree vlan 4 port-priority 10</code>                    | Assign the port priority of 10 for VLAN 4.   |
| Step 25 | <code>spanning-tree vlan 5 port-priority 10</code>                    | Assign the port priority of 10 for VLAN 5.   |
| Step 26 | <code>spanning-tree vlan 6 port-priority 10</code>                    | Assign the port priority of 10 for VLAN 6.   |
| Step 27 | <code>end</code>  | Return to privileged EXEC mode.  |
| Step 28 | <code>show running-config</code>                                      | Verify your entries.   |
| Step 29 | <code>copy running-config startup-config</code>                       | (Optional) Save your entries in the configuration file.  |

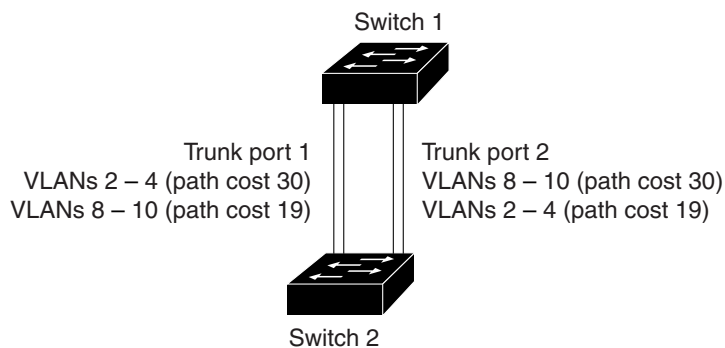
## Load Sharing Using STP Path Cost

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. The VLANs keep the traffic separate. Because no loops exist, STP does not disable the ports, and redundancy is maintained in the event of a lost link.

In [Figure 9-6](#), Trunk ports 1 and 2 are 100BASE-T ports. The path costs for the VLANs are assigned as follows:

- 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 9-6** Load-Sharing Trunks with Traffic Distributed by Path Cost



## Configuring STP Path Costs and Load Sharing

Beginning in privileged EXEC mode, follow these steps to configure the network shown in [Figure 9-6](#):

|        | Command   | Purpose   |
|--------|---|---|
| Step 1 | <code>configure terminal</code>                                       | Enter global configuration mode on Switch 1.  |
| Step 2 | <code>interface fastethernet 0/1</code>                               | Enter interface configuration mode, and define Fast Ethernet port 0/1 as the interface to be configured as a trunk.                     |
| Step 3 | <code>switchport trunk encapsulation {isl   dot1q   negotiate}</code> | Configure the port to support ISL or 802.1Q encapsulation.<br>You must configure each end of the link with the same encapsulation type. |
| Step 4 | <code>switchport mode trunk</code>                                    | Configure the port as a trunk port.<br>The trunk defaults to ISL trunking.  |
| Step 5 | <code>exit</code>   | Return to global configuration mode.  |
| Step 6 |   | Repeat Steps 2 through 4 on Switch 1 interface Fast Ethernet 0/2.   |
| Step 7 | <code>end</code>  | Return to privileged EXEC mode.   |

|         | Command   | Purpose   |
|---------|---|---|
| Step 8  | <code>show running-config</code>                | Verify your entries.<br>In the display, make sure that interfaces Fast Ethernet 0/1 and Fast Ethernet 0/2 are configured as trunk ports.              |
| Step 9  | <code>show vlan</code>                          | When the trunk links come up, Switch 1 receives the VTP information from the other switches. Verify that Switch 1 has learned the VLAN configuration. |
| Step 10 | <code>configure terminal</code>                 | Enter global configuration mode.  |
| Step 11 | <code>interface fastethernet 0/1</code>         | Enter interface configuration mode, and define Fast Ethernet port 0/1 as the interface to set the STP cost.   |
| Step 12 | <code>spanning-tree vlan 2 cost 30</code>       | Set the spanning-tree path cost to 30 for VLAN 2.   |
| Step 13 | <code>spanning-tree vlan 3 cost 30</code>       | Set the spanning-tree path cost to 30 for VLAN 3.   |
| Step 14 | <code>spanning-tree vlan 4 cost 30</code>       | Set the spanning-tree path cost to 30 for VLAN 4.   |
| Step 15 | <code>end</code>                                | Return to global configuration mode.  |
| Step 16 |   | Repeat Steps 9 through 11 on Switch 1 interface Fast Ethernet 0/2, and set the spanning-tree path cost to 30 for VLANs 8, 9, and 10.                  |
| Step 17 | <code>exit</code>                               | Return to privileged EXEC mode.   |
| Step 18 | <code>show running-config</code>                | Verify your entries.<br>In the display, verify that the path costs are set correctly for interfaces Fast Ethernet 0/1 and 0/2.                        |
| Step 19 | <code>copy running-config startup-config</code> | (Optional) Save your entries in the configuration file.   |

## Understanding VMPS

The Catalyst 3550 switch acts as a client to the VMPS and communicates with it through the VLAN Query Protocol (VQP). When the VMPS receives a VQP request from a client switch, 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 secure mode. Secure mode determines whether the server shuts down the port when a VLAN is not allowed on it or just denies the port access to the VLAN.

In response to a request, the VMPS takes one of these actions:

- If the assigned VLAN is restricted to a group of ports, the VMPS verifies the requesting port against this group and responds as follows:
  - If the VLAN is allowed on the port, the VMPS sends the VLAN name to the client in response.
  - If the VLAN is not allowed on the port and the VMPS is not in secure 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 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 receives an *access-denied* response from the VMPS, it continues to block traffic from the MAC address to or from the port. The switch continues to monitor the packets directed to the port and sends a query to the VMPS when it identifies a new address. If the switch receives a *port-shutdown* response from the VMPS, it disables the port. The port must be manually re-enabled by using the CLI, CMS, or SNMP.

You can also use an explicit entry in the configuration table to deny access to specific MAC addresses for security reasons. If you enter the **none** keyword for the VLAN name, the VMPS sends an *access-denied* or *port-shutdown* response, depending on the VMPS secure mode setting.

## Dynamic Port VLAN Membership

A dynamic (nontrunking) port on the switch can belong to only one VLAN. When the link comes up, the switch 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 port and attempts to match the MAC address to a VLAN in the VMPS database.

If there is a match, the VMPS sends the VLAN number for that port. If the client switch 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 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 port if they are all in the same VLAN; however, the VMPS shuts down a dynamic port if more than 20 hosts are active on the port.

If the link goes down on a dynamic 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.

## VMPS Database Configuration File

The VMPS contains a database configuration file that you create. This ASCII text file is stored on a switch-accessible TFTP server that functions as a VMPS server. The file contains VMPS information, such as the domain name, the fallback VLAN name, and the MAC-address-to-VLAN mapping. The Catalyst 3550 switch cannot act as the VMPS, but you can use a Catalyst 5000 or Catalyst 6000 series switch as the VMPS.

You can configure a fallback VLAN name. If you connect a device with a MAC address that is not in the database, the VMPS sends the fallback VLAN name to the client. If you do not configure a fallback VLAN and the MAC address does not exist in the database, the VMPS sends an *access-denied* response. If the VMPS is in secure mode, it sends a *port-shutdown* response.

Whenever port names are used in the VMPS database configuration file, the server must use the switch convention for naming ports. For example, Gi0/4 is fixed Gigabit Ethernet port number 4. If the switch is a cluster member, the command switch adds the name of the switch before the type. For example, *es3%Gi0/4* refers to fixed Gigabit Ethernet port 4 on member switch 3. When port names are required, these naming conventions must be followed in the VMPS database configuration file when it is configured to support a cluster.

This example shows an example of a VMPS database configuration file as it appears on a Catalyst 6000 series switch. The file has these characteristics:

- The security mode is open.
- The default is used for the fallback VLAN.
- MAC address-to-VLAN name mappings—The MAC address of each host and the VLAN to which each host belongs is defined.
- Port groups are defined.
- VLAN groups are defined.
- VLAN port policies are defined for the ports associated with restricted VLANs.

```
!VMPS File Format, version 1.1
! Always begin the configuration file with
! the word "VMPS"
!
!vmps domain <domain-name>
! The VMPS domain must be defined.
!vmps mode {open | secure}
! The default mode is open.
!vmps fallback <vlan-name>
!vmps no-domain-req { allow | deny }
!
! The default value is allow.
vmps domain DSBU
vmps mode open
vmps fallback default
vmps no-domain-req deny
!
!
!MAC Addresses
!
vmps-mac-addr
!
! address <addr> vlan-name <vlan_name>
!
address 0012.2233.4455 vlan-name hardware
address 0000.6509.a080 vlan-name hardware
address aabb.ccdd.eeff vlan-name Green
address 1223.5678.9abc vlan-name ExecStaff
address fedc.ba98.7654 vlan-name --NONE--
address fedc.ba23.1245 vlan-name Purple
!
!Port Groups
!
!vmps-port-group <group-name>
! device <device-id> { port <port-name> | all-ports }
!
vmps-port-group WiringCloset1
device 198.92.30.32 port 0/2
device 172.20.26.141 port 0/8
vmps-port-group "Executive Row"
device 198.4.254.222 port 0/2
device 198.4.254.222 port 0/3
device 198.4.254.223 all-ports
!
!
!VLAN groups
!
!vmps-vlan-group <group-name>
! vlan-name <vlan-name>
```

```

!
vmps-vlan-group Engineering
vlan-name hardware
vlan-name software
!
!
!VLAN port Policies
!
!vmps-port-policies {vlan-name <vlan_name> | vlan-group <group-name> }
! { port-group <group-name> | device <device-id> port <port-name> }
!
vmps-port-policies vlan-group Engineering
port-group WiringCloset1
vmps-port-policies vlan-name Green
device 198.92.30.32 port 0/8
vmps-port-policies vlan-name Purple
device 198.4.254.22 port 0/2
port-group "Executive Row"

```

## VMPS Configuration Guidelines

These guidelines and restrictions apply to dynamic port VLAN membership:

- You must configure the VMPS before you configure ports as dynamic.
- The communication between a cluster of switches and VMPS is managed by the command switch and includes port-naming conventions that are different from standard port names. For the cluster-based port-naming conventions, see the [“VMPS Database Configuration File” section on page 9-34](#).
- When you configure a port as dynamic, the spanning-tree Port Fast feature is automatically enabled for that port. The Port Fast mode accelerates the process of bringing the port into the forwarding state. You can disable Port Fast mode on a dynamic port.
- 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 ports, but you can enter the **switchport access vlan dynamic** interface configuration command for a trunk port. In this case, the switch 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 ports cannot be monitor ports.
- Dynamic ports cannot be members of an EtherChannel group.
- A dynamic access port can participate in fallback bridging.
- The VTP management domain of the VMPS client and the VMPS server must be the same.

## Default VMPS Configuration

Table 9-9 shows the default VMPS and dynamic port configuration on client switches.

**Table 9-9** Default VMPS Client and Dynamic Port Configuration

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

## Configuring an Interface as a Layer 2 Dynamic Access Port

You configure dynamic VLANs by using the VMPS (server). The switch cannot be a VMPS server; the server can be a Catalyst 6000 switch or other similar device.

### Entering the IP Address of the VMPS

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



**Note**

If the VMPS is being defined for a cluster of switches, enter the address on the command switch.

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

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

This is an example of output for the **show vmps** privileged EXEC command, used to verify the VMPS server IP address.

```
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:          No Dynamic Port
```

**Note**

The switch port that is connected to the VMPS server cannot be a dynamic access port. It can be either a static access port or a trunk port. See the [“Configuring an Ethernet Interface as a Trunk Port” section on page 9-25](#).

## Configuring Dynamic Access Ports on VMPS Clients

**Caution**

Dynamic port VLAN membership is for end stations or hubs connected to end stations. Connecting dynamic access ports to other switches 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:

|        | Command  | Purpose   |
|--------|--|---|
| Step 1 | <b>configure terminal</b>                                    | Enter global configuration mode.  |
| Step 2 | <b>interface</b> <i>interface-id</i>                         | Enter interface configuration mode and the switch port that is connected to the end station.                                |
| Step 3 | <b>switchport mode access</b>                                | Set the port to access mode.  |
| Step 4 | <b>switchport access vlan dynamic</b>                        | Configure the port as eligible for dynamic VLAN membership.<br>The dynamic access port must be connected to an end station. |
| Step 5 | <b>end</b>   | Return to privileged EXEC mode.   |
| Step 6 | <b>show interfaces</b> <i>interface-id</i> <b>switchport</b> | Verify your entries in the <i>Operational Mode</i> field of the display.  |
| Step 7 | <b>copy running-config startup-config</b>                    | (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 return an interface to its default switchport mode (dynamic desirable), use the **no switchport mode** interface configuration command. To reset the access mode to the default VLAN for the switch, use the **no switchport access** interface configuration command.

## Reconfirming VLAN Memberships

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

|        | Command                | Purpose  |
|--------|------------------------|--|
| Step 1 | <b>vmpls reconfirm</b> | Reconfirm dynamic port VLAN membership.        |
| Step 2 | <b>show vmpls</b>      | Verify the dynamic VLAN reconfirmation status. |

## 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.

If you are configuring a member switch in a cluster, this parameter must be equal to or greater than the reconfirmation setting on the command switch.

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

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

To return the switch to its default setting, use the **no vmpls 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 attempts to contact the VMPS before querying the next server:

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

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

## Administering and Monitoring the VMPS

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

|                    |   |
|--------------------|---|
| VMPS VQP Version   | The version of VQP used to communicate with the VMPS. The switch queries the VMPS that is using VQP version 1.  |
| Reconfirm Interval | The number of minutes the switch 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 starts to query the secondary VMPS.   |
| VMPS domain server | The IP address of the configured VLAN membership policy servers. The switch sends queries to the one marked <i>current</i> . The one marked <i>primary</i> 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 <b>vmps reconfirm</b> privileged EXEC command or its CMS or SNMP equivalent. |

## Troubleshooting Dynamic Port VLAN Membership

The VMPS shuts down a dynamic 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 port.

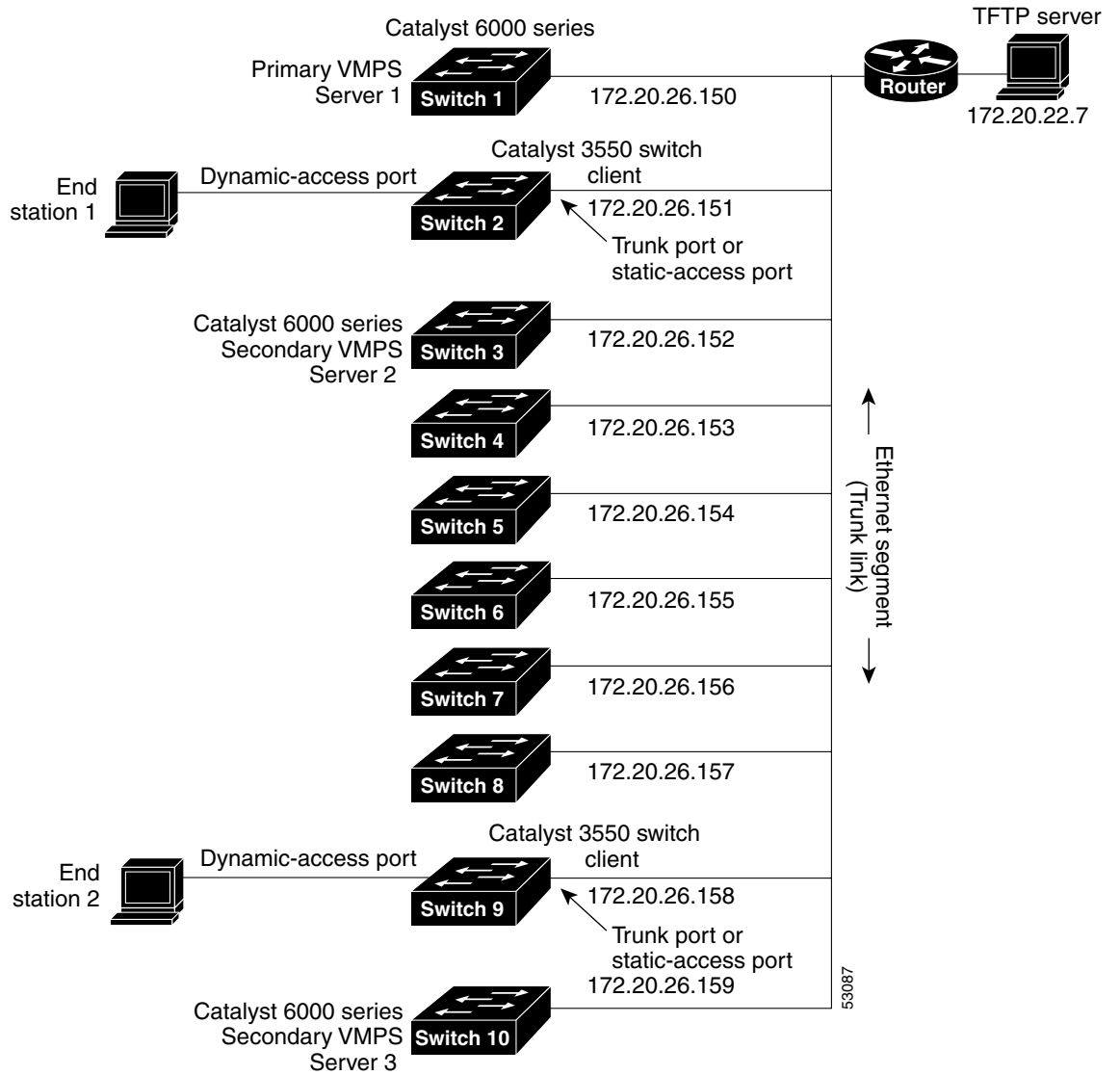
To re-enable a disabled dynamic port, enter the **no shutdown** interface configuration command.

## Dynamic Port VLAN Membership Configuration Example

Figure 9-7 shows a network with a VMPS server switch and VMPS client switches with dynamic ports. In this example, these assumptions apply:

- The VMPS server and the VMPS client are separate switches.
- The Catalyst 6000 series Switch 1 is the primary VMPS server.
- The Catalyst 6000 series Switch 3 and Switch 10 are secondary VMPS servers.
- End stations are connected to the Catalyst 3550 clients, Switch 2 and Switch 9.
- The database configuration file is stored on the TFTP server with the IP address 172.20.22.7.

Figure 9-7 Dynamic Port VLAN Membership Configuration



78035

