

Configuring VTP and Virtual LANs

This chapter describes how Virtual Trunk Protocol (VTP) works, how you configure it, and how you add VLANs to a VLAN network managed by VTP. For complete syntax and usage information on the commands described in this chapter, refer to the *Cisco IOS Desktop Switching Command Reference* (online only).

Note Different switches can support different numbers of VLANs. See Table 1-1 in Chapter 1, “Overview,” for a complete list of the switches and their VLAN support.

These sections describe how to configure VTP and VLANs:

- “How VTP Works” section on page 2-2
- “Configuring VTP” section on page 2-8
- “How VLANs Work” section on page 2-18
- “Configuring VLANs” section on page 2-25
- “How QoS Works” section on page 2-32
- “Setting the Port Priority for CoS Values” section on page 2-36

How VTP Works

Before you create VLANs, you must decide whether to use VTP in your network. Using VTP, you can make configuration changes centrally on a single switch, such as a 2900 XL switch, 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.

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.

The VTP Domain

A VTP domain (also called a VLAN management domain) is one switch or several interconnected switches sharing the same VTP domain. A switch is configured to be in only one VTP domain. You make global VLAN configuration changes for the domain by using the CLI, Cisco Visual Switch Manager (CVSM) software, or Simple Network Management Protocol (SNMP).

By default, a 2900 or 3500 XL switch is in the no-management-domain state until it receives an advertisement for a domain over a trunk link or you configure a management domain. The default VTP mode is server mode, but VLANs are not propagated over the network until a management domain name is specified or learned.

If the switch receives a VTP advertisement over a trunk link, it inherits the management domain name and configuration revision number. The switch then ignores advertisements with a different management 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), IEEE 802.1Q, IEEE 802.10, and Asynchronous Transfer Mode (ATM) LAN Emulation (LANE).

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

Upgrading the Switch Software

When you upgrade from a software version that supports VLANs but does not support VTP, such as Cisco IOS Release 11.2(8)SA3, to a version that does support VTP, ports that belong to a VLAN retain their VLAN membership, and VTP enters transparent mode. The domain name becomes UPGRADE, and VTP does not propagate the VLAN configuration to other switches.

If you want to propagate the VLAN configuration to other switches, configure the switch to operate as a VTP server, and change the domain name.

VTP Modes and VTP Mode Transitions

You can configure a supported switch to be in one of the following VTP modes:

- **VTP server**—In this mode, you can create, modify, and delete VLANs and specify other configuration parameters (such as 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.

In VTP server mode, VLAN configurations are saved in nonvolatile memory. VTP server is the default mode.

- **VTP client**—In this mode, VTP clients behave like VTP servers, but you cannot create, change, or delete VLANs on a VTP client.

In VTP client mode, VLAN configurations are not saved in nonvolatile memory.

- **VTP transparent**—In this mode, 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, transparent switches do forward VTP advertisements that they receive from other switches. You can create, modify, and delete VLANs.

In VTP transparent mode, VLAN configurations are saved in nonvolatile memory, but they are not advertised to other switches.

Two configurations can cause a switch running this version of software to automatically change VTP mode:

- When the network is configured with more than 250 VLANs, the switch automatically changes from VTP server or client mode to VTP transparent mode. The switch then operates with the VLAN configuration that preceded the one that sent it into transparent mode.
- When a multi-VLAN port is configured on a supported switch in VTP server mode or client mode, the switch automatically changes to transparent mode.

The “VTP Configuration Guidelines” section on page 2-7 provides tips and caveats for configuring VTP.

VTP Advertisements

Each switch in the VTP domain sends these 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.

The following global domain information is distributed in VTP advertisements:

- VTP domain name
- VTP configuration revision number
- Update identity and update timestamp
- MD5 digest

The following VLAN information is distributed in VTP advertisements for each configured VLAN:

- VLAN ID
- 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 VTP version 1 or version 2. If your environment has Token Ring networks, you must use version 2.

VTP version 2 supports the following features not supported in version 1:

- **Token Ring support**—VTP version 2 supports Token Ring LAN switching and VLANs (Token Ring Bridge Relay Function [TrBRF] and Token Ring Concentrator Relay Function [TrCRF]). For more information about Token Ring VLANs, refer to the “How VLANs Work” section on page 2-18.
- **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 nonvolatile memory 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 only one domain is supported in the Enterprise Edition Software, VTP version 2 forwards VTP messages in transparent mode without checking 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 CVSM software, or SNMP. Consistency checks are not performed when new information is obtained from a VTP message or when information is read from nonvolatile memory. If the digest on a received VTP message is correct, its information is accepted without consistency checks.

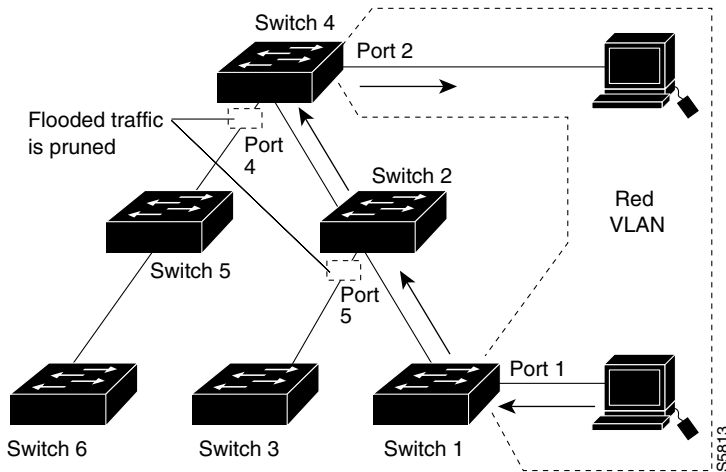
VTP Pruning

Although switches supported by this IOS release are never eligible for VTP pruning, a supported switch does propagate VTP pruning messages. This section describes the role that a supported switch can play in a VTP pruning network.

VTP pruning increases available bandwidth by restricting flooded traffic to those trunk links that the traffic must use to access the appropriate network devices. When VTP pruning is enabled, it can block flooded traffic to VLANs that are included in the pruning-eligible list. Switches supported by this IOS release are never in the pruning-eligible list, and no switch traffic is pruned. Flooding occurs as usual, and switches connected to the supported switch do not benefit from pruning.

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

Figure 2-1 Flooding Traffic with VTP Pruning



VTP Configuration Guidelines

Follow these guidelines when implementing VTP in your network:

- All switches in a VTP domain must run the same VTP version.
- The password entered with a domain name should be the same for all switches in the domain.



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

- A VTP version 2-capable switch can operate in the same VTP domain as a switch running VTP version 1 provided 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 will not exchange VTP information with switches with version 2 enabled.
- If there are Token Ring networks in your environment (TrBRF and TrCRF), 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 management domain.

Default VTP Configuration

Table 2-1 shows the default VTP configuration.

Table 2-1 VTP Default Configuration

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

Configuring VTP

You configure VTP by entering commands from the VLAN database configuration command mode. You display the status of VTP by entering the privileged EXEC mode **show vtp status** command.

When you enter the **exit** command in VLAN database mode, it applies to all the commands that you entered. VTP messages are sent to other switches in the management domain, and you are returned to privileged EXEC mode.

For more information about these commands, refer to the *Cisco IOS Desktop Switching Command Reference*.

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

Configuring a VTP Server

When a switch is in VTP server mode, you can change the VLAN configuration and have it propagate throughout the network. To configure the switch as a VTP server, perform this task from privileged EXEC mode:

Task	Command
Step 1 Enter VLAN configuration mode.	vlan database
Step 2 Configure a VTP administrative-domain name. This can be from 1 to 32 characters.	vtp domain <i>domain-name</i>
Step 3 (Optional) Set a password for the VTP domain. The password can be from 8 to 64 characters.	vtp password <i>password-value</i>
Step 4 Configure the switch as a server.	vtp server
Step 5 Return to privileged EXEC mode.	exit
Step 6 Verify the VTP configuration.	show vtp status

Configuring VTP

This example shows how to enter a VTP domain name and configure the switch as a VTP server:

```
Switch# vlan database
Switch(vlan)# vtp domain Building_A
Setting VTP domain name to Building_A
Switch(vlan)# vtp domain Building_A password LAVA
Domain name already set to Building_A .
Setting device VLAN database password to LAVA.
Switch(vlan)# vtp server
Setting device to VTP SERVER mode.
Switch(vlan)# exit
APPLY completed.
Exiting....
```

```
Switch# show vtp status
VTP Version                : 2
Configuration Revision     : 0
Maximum VLANs supported locally : 68
Number of existing VLANs   : 6
→ VTP Operating Mode       : Server
→ VTP Domain Name         : Building_A
VTP Pruning Mode           : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation       : Disabled
MD5 digest                  : 0x09 0xF6 0x57 0x1C 0xC9 0x6F 0x75 0x16
```

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 management domain and then modifies its configuration accordingly.

To configure the switch as a VTP client, perform this task from privileged EXEC mode:

Task	Command
Step 1 Enter VLAN configuration mode.	vlan database
Step 2 Place the switch in VTP client mode.	vtp client
Step 3 Update the VLAN database, propagate it throughout the administrative domain, and return to privileged EXEC mode.	exit
Step 4 Verify the VTP configuration.	show vtp status

This example shows how to configure the switch as a VTP client and verify the configuration:

```
Switch# vlan database
Switch(vlan)# vtp client
Setting device to VTP CLIENT mode.
```

```
Switch(vlan)# exit
In CLIENT state, no apply attempted.
Exiting....
```

```
Switch# show vtp status
VTP Version                : 2
Configuration Revision     : 0
Maximum VLANs supported locally : 68
Number of existing VLANs   : 6
→ VTP Operating Mode       : Client
VTP Domain Name            : Building_A
VTP Pruning Mode           : Disabled
VTP V2 Mode                : Disabled
VTP Traps Generation       : Disabled
MD5 digest                  : 0x09 0xF6 0x57 0x1C 0xC9 0x6F 0x75 0x16
Configuration last modified by 172.20.130.40 at 3-5-93 22:15:25
```

Disabling VTP

When you configure the switch as VTP transparent, 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 does forward received VTP advertisements on all of its trunk links.

To put the switch in VTP transparent mode, perform this task from privileged EXEC mode:

Task	Command
Step 1 Enter VLAN configuration mode.	vlan database
Step 2 Place the switch in VTP transparent mode (disabling VTP on the switch).	vtp transparent
Step 3 Return to privileged EXEC mode.	exit
Step 4 Verify the VTP configuration.	show vtp status

This example shows how to configure the switch as VTP transparent and verify the configuration:

```
Switch# vlan database
Switch(vlan)# vtp transparent
Setting device to VTP TRANSPARENT mode.
```

```
Switch(vlan)# exit
APPLY completed.
Exiting....
```

```
Switch# show vtp status
VTP Version                : 2
Configuration Revision     : 0
Maximum VLANs supported locally : 68
Number of existing VLANs   : 6
→ VTP Operating Mode       : Transparent
VTP Domain Name            : Building_A
VTP Pruning Mode           : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation       : Disabled
MD5 digest                  : 0x09 0xF6 0x57 0x1C 0xC9 0x6F 0x75 0x16
Configuration last modified by 172.20.130.40 at 3-5-93 22:15:25
```

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 a Token Ring environment, you must enable VTP version 2 for Token Ring VLAN switching to function properly.

To enable VTP version 2, perform this task from privileged EXEC mode:

Task	Command
Step 1 Enter VLAN configuration mode.	vlan database
Step 2 Enable VTP version 2 on the switch.	vtp v2-mode
Step 3 Update the VLAN database, propagate it throughout the administrative domain, and return to privileged EXEC mode.	exit
Step 4 Verify that VTP version 2 is enabled.	show vtp status

This example shows how to enable VTP version 2 and verify the configuration:

```
Switch# vlan database
Switch(vlan)# vtp v2-mode
V2 mode enabled.
Switch(vlan)# exit
APPLY completed.
Exiting....
```

```
Switch# show vtp status
VTP Version                : 2
Configuration Revision     : 2
Maximum VLANs supported locally : 68
Number of existing VLANs   : 14
VTP Operating Mode         : Server
VTP Domain Name            : milano
VTP Pruning Mode           : Disabled
→ VTP V2 Mode              : Enabled
VTP Traps Generation       : Disabled
MD5 digest                 : 0xAC 0x23 0x2F 0x75 0x52 0xDC 0x17 0x70
Configuration last modified by 172.20.128.178 at 3-6-93 23:46:53
```

Disabling VTP Version 2

To disable VTP version 2, perform this task from privileged EXEC mode:

Task	Command
Step 1 Enter VLAN configuration mode.	vlan database
Step 2 Disable VTP version 2.	no vtp v2-mode
Step 3 Update the VLAN database, propagate it throughout the administrative domain, and return to privileged EXEC mode.	exit
Step 4 Verify that VTP version 2 is disabled.	show vtp status

This example shows how to disable VTP version 2:

```
Switch# vlan database
Switch(vlan)# no vtp v2-mode
V2 mode disabled.
Switch(vlan)# exit
In CLIENT state, no apply attempted.
Exiting....

Switch# show vtp status
VTP Version                : 2
Configuration Revision     : 0
Maximum VLANs supported locally : 68
Number of existing VLANs   : 59
VTP Operating Mode         : Client
VTP Domain Name            : milano
VTP Pruning Mode          : Disabled
VTP V2 Mode                : Disabled
VTP Traps Generation       : Disabled
MD5 digest                 : 0x53 0x97 0x06 0x02 0xF8 0x6F 0x45 0x85
Configuration last modified by 172.20.128.151 at 3-5-93 01:05:21
```



Monitoring VTP

You monitor VTP by displaying its 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.

To monitor VTP activity, perform this task from privileged EXEC mode:

Task	Command
Step 1 Display the VTP switch configuration information.	show vtp status
Step 2 Display counters about VTP messages being sent and received.	show vtp counters

This example shows how to display the switch VTP status:

```
Switch# show vtp status
VTP Version                : 2
Configuration Revision     : 2
Maximum VLANs supported locally : 68
Number of existing VLANs   : 6
VTP Operating Mode         : Transparent
VTP Domain Name            : Building_A
VTP Pruning Mode           : Disabled
VTP V2 Mode                : Disabled
VTP Traps Generation       : Disabled
MD5 digest                  : 0xB9 0xC7 0x8D 0xB3 0xD4 0xBA 0x94 0x03
Configuration last modified by 172.20.130.40 at 3-9-93 20:12:24
```

This example shows how to display the VTP statistics:

```
Switch# show vtp counters
```

```
VTP statistics:
```

```
Summary advertisements received : 3
Subset advertisements received  : 2
Request advertisements received  : 0
Summary advertisements transmitted : 10
Subset advertisements transmitted : 10
Request advertisements transmitted : 1
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
-----	-----	-----	-----
Fa1/1	8	6	0
Fa1/2	6	0	0
Fa1/3	6	0	0
Fa1/4	6	0	0

How VLANs Work

A VLAN is a group of end stations with a common set of requirements, independent of physical location. VLANs have the same attributes as a physical LAN, but you can group end stations even if they are not physically located on the same LAN segment.

VLANs on supported switches and other supported devices limit unicast, multicast, and broadcast traffic flooding. Flooded traffic originating from a particular VLAN is only flooded out other ports belonging to that VLAN.

Clusters

Cisco IOS Release 12.0(5)XP supports the grouping of switches into clusters. A cluster is up to 16 switches that can be managed as a single entity. The *command* switch is the single point of management for the cluster. *Member* switches are managed through the command switch.

Switches in a cluster can be connected through ports that belong to any VLAN that is configured as the management VLAN.

Adding VLANs to a Cluster

If you are configuring VLANs on a member switch, you might need to enter an extra command from the command switch CLI to access the member switch. When configuring port parameters, for example, you can use the privileged EXEC **rcommand** command and the number of the member switch to display the member switch CLI. Once you have accessed the member switch, command mode changes and IOS commands operate as usual. Enter **exit** on the member switch in privileged EXEC mode to return to the command switch CLI.

See the *Cisco IOS Desktop Switching Software Configuration Guide* and the *Cisco IOS Desktop Switching Command Reference* for more information on managing clusters.

VLAN Membership

Ports that belong to VLANs are configured with a membership mode that determines what kind of traffic each port carries and how many VLANs it can belong to. Table 2-2 lists the membership modes and characteristics.

Table 2-2 Port Membership Modes

Membership Mode	VLAN Membership Characteristics
Static-access	Can belong to one VLAN and is manually assigned. This is the default.
Multi-VLAN	Can belong to up to 250 VLANs (some models only support 64 VLANs) and is manually assigned. A multi-VLAN port cannot be configured when there is a trunk configured on the switch. VLAN traffic on the multi-VLAN port is not encapsulated.
Dynamic access	Can belong to one VLAN and is dynamically assigned by a VLAN Membership Policy Server (VMPS).
Trunk (ISL, ATM, or IEEE 802.1Q)	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.

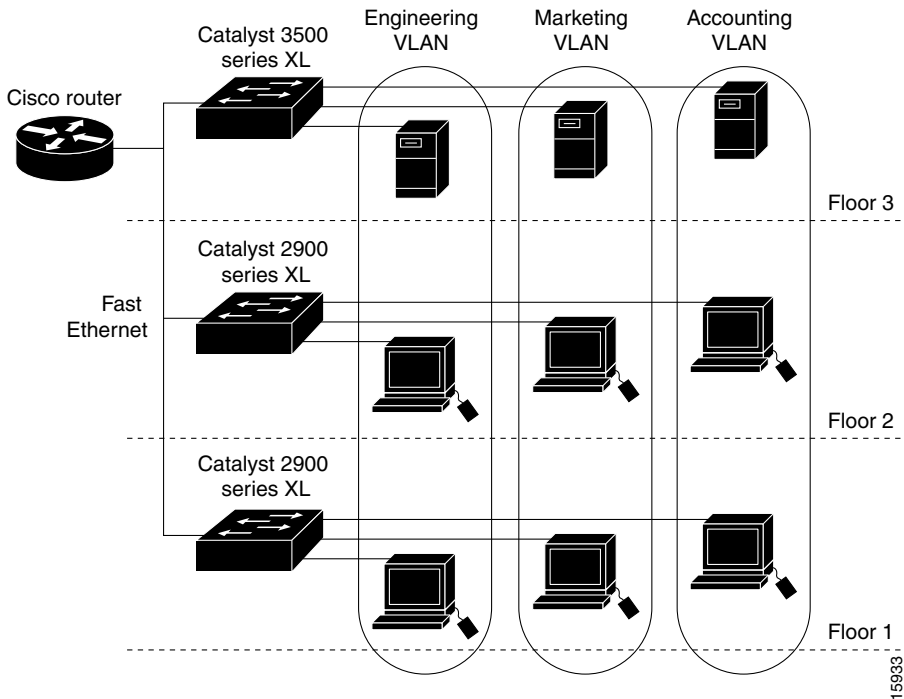
VLANs in a VTP Domain

Before you create VLANs, you must decide whether to use VTP to maintain global VLAN configuration information for your network. For complete information on VTP, refer to the “How VTP Works” section on page 2-2.

Figure 2-2 shows an example of VLANs segmented into 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. Traffic between VLANs must be routed. Port VLAN membership on the switch is assigned manually on a port-by-port basis. Ports assigned to a VLAN by this method are said to have port-based, or static, VLAN membership.

Figure 2-2 VLANs as Logically Defined Networks



15933

You can set the following parameters when you add a VLAN to a 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 Configurations” section on page 2-22 lists the default values and possible ranges for each VLAN media type.

Token Ring VLANs

Although the 2900 and 3500 XL 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 this IOS release advertise information about Token Ring VLANs when running VTP version 2. The following Token Ring VLAN types are supported on the supported switches running VTP version 2:

- Token Ring TrBRF VLANs
- Token Ring TrCRF VLANs

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

VLAN Configuration Guidelines

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

- A maximum of 250 VLANs can be active on supported switches, and some models only support 64 switches. If VTP reports that there are 254 active VLANs, 4 of the active VLANs (1002 to 1005) are reserved for Token Ring and FDDI.
- Before you can create a VLAN, the switch must be in VTP server mode or VTP transparent mode. For information on configuring VTP, refer to the “Configuring VTP” section on page 2-8.
- Switches running this IOS release 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 via VTP.

Default VLAN Configurations

Table 2-3 through Table 2-7 shows the default configurations for the different VLAN media types.

Note Catalyst 2900 XL switches support Ethernet interfaces exclusively. Because FDDI and Token Ring VLANs are not locally supported, you configure FDDI and Token Ring media-specific characteristics only for VTP global advertisements to other switches.

Table 2-3 Ethernet VLAN Defaults and Ranges

Parameter	Default	Range
VLAN ID	1	1–1005
VLAN name	VLANxxxx, where xxxx is the VLAN ID	No range
802.10 SAID	100000+VLAN ID	1–4294967294
MTU size	1500	1500–18190
Translational bridge 1	0	0–1005
Translational bridge 2	0	0–1005
VLAN state	active	active, suspend

Table 2-4 FDDI VLAN Defaults and Ranges

Parameter	Default	Range
VLAN ID	1002	1–1005
VLAN name	VLANxxxx, where xxxx is the VLAN ID	No range
802.10 SAID	100000+VLAN ID	1–4294967294
MTU size	1500	1500–18190
Ring number	None	1–4095
Parent VLAN	0	0–1005
Translational bridge 1	0	0–1005
Translational bridge 2	0	0–1005
VLAN state	active	active, suspend

Table 2-5 FDDI-Net VLAN Defaults and Ranges

Parameter	Default	Range
VLAN ID	1004	1–1005
VLAN name	VLANxxxx, where xxxx is the VLAN ID	No range
802.10 SAID	100000+VLAN ID	1–4294967294
MTU size	1500	1500–18190
Bridge number	0	0–15
STP type	ieee	auto, ibm, ieee
Translational bridge 1	0	0–1005
Translational bridge 2	0	0–1005
VLAN state	active	active, suspend

Table 2-6 Token Ring (TrBRF) VLAN Defaults and Ranges

Parameter	Default	Range
VLAN ID	1005	1–1005
VLAN name	VLANxxxx, where xxxx is the VLAN ID	No range
802.10 SAID	100000+VLAN ID	1–4294967294
MTU size	VTPv1 1500; VTPv2 4472	1500–18190
Bridge number	VTPv1 0; VTPv2 user-specified	0–15
STP type	ibm	auto, ibm, ieee
Translational bridge 1	0	0–1005
Translational bridge 2	0	0–1005
VLAN state	active	active, suspend

Table 2-7 Token Ring (TrCRF) VLAN Defaults and Ranges

Parameter	Default	Range
VLAN ID	1003	1–1005
VLAN name	VLANxxxx, where xxxx is the VLAN ID	No range
802.10 SAID	100000+VLAN ID	1–4294967294
Ring Number	VTPv1 default 0; VTPv2 user-specified	1–4095
Parent VLAN	VTPv1 default 0; VTPv2 user-specified	0–1005
MTU size	VTPv1 default 1500; VTPv2 default 4472	1500–18190
Translational bridge 1	0	0–1005
Translational bridge 2	0	0–1005
VLAN state	active	active, suspend
Bridge mode	srb	srb, srt
ARE max hops	7	0–13
STE max hops	7	0–13
Backup CRF	disabled	disable; enable

Configuring VLANs

You use the VLAN database command mode to add, change, and delete VLANs. 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 privileged EXEC mode **show vlan** command. The `vlan.dat` file is stored in nonvolatile memory. The `vlan.dat` file is upgraded automatically, but you cannot go back to an earlier version of Cisco IOS after you upgrade to this release.



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 commands described in the *Cisco IOS Desktop Switching Command Reference*.

You use the interface configuration command mode to define the port membership mode and add and remove ports from VLAN. The results of these commands are written to the running-configuration file, and you can display the file by entering the privileged EXEC mode **show running-config** 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 *Cisco IOS Desktop Switching Command Reference*.

Adding an Ethernet VLAN

Each 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. See the “Default VLAN Configurations” section on page 2-22 for the list of default parameters that are assigned when you add a VLAN.

If you do not specify the VLAN type, the VLAN is an Ethernet VLAN. To add a VLAN, perform this task from privileged EXEC mode:

Task	Command
Step 1 Enter VLAN configuration mode.	vlan database
Step 2 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.	vlan <i>vlan-id</i> name <i>vlan-name</i>
Step 3 Update the VLAN database, propagate it throughout the administrative domain, and return to privileged EXEC mode.	exit
Step 4 Verify the VLAN configuration.	show vlan name <i>vlan-name</i>

This example shows how to create an Ethernet VLAN and verify the configuration:

```
Switch# vlan database
Switch(vlan)# vlan 0003 name marketing
VLAN 3 added:
      Name: marketing
Switch(vlan)# exit
APPLY completed.
Exiting....

Switch# show vlan name marketing
VLAN Name                               Status      Ports
-----
3      marketing                             active

VLAN Type  SAID      MTU    Parent RingNo BridgeNo Stp    Trans1  Trans2
-----
3      enet    100003   1500   -      -      -      -      0      0
```

Modifying an Ethernet VLAN

The following task table illustrates how to modify VLAN parameters. You must perform this task from privileged EXEC mode:

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

Configuring VLANs

This example shows how to modify an Ethernet VLAN and verify the configuration:

```
Switch# vlan database
Switch(vlan)# vlan 0003 mtu 4000
VLAN 3 modified:
      MTU 4000
```

```
Switch(vlan)# exit
APPLY completed.
Exiting....
```

```
Switch# show vlan 0003
```

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	Trans1	Trans2
3	enet	100003	4000	-	-	-	-	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.

To delete a VLAN on the switch, perform this task from privileged EXEC mode:

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

Configuring VLANs

This example shows how to delete a VLAN:

```
Switch# vlan database
Switch(vlan)# no vlan 3
Deleting VLAN 3...
Switch(vlan)# exit
APPLY completed.
Exiting....
```

```
Switch# show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16
2 VLAN0002	active	
4 VLAN0004	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

A static-access port belongs to one VLAN. To assign a port to a VLAN, perform this task from privileged EXEC mode:

Note If you are assigning a port on a cluster member switch to a VLAN, first log in to the member switch by using the privileged EXEC **rcommand** command. See the *Cisco IOS Desktop Switching Command Reference* for more information on how to use this command.

Task	Command
Step 1 Enter global configuration mode.	configure terminal
Step 2 Enter interface configuration mode, and define the interface to be added to the VLAN.	interface <i>interface</i>
Step 3 Define the VLAN membership mode for this port.	switchport mode access
Step 4 Assign the port to the VLAN.	switchport access vlan 3
Step 5 Return to privileged EXEC mode.	exit
Step 6 Verify the VLAN configuration.	show interface <i>interface-id</i> switchport

This example shows how to assign switch ports to a VLAN and verify the assignment:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface fa0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 0003
Switch(config-if)# end

Switch# show interface fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative mode: static access
→ Operational Mode: static access
Administrative Trunking Encapsulation: isl
Operational Trunking Encapsulation: isl
→ Negotiation of Trunking: Disabled
Access Mode VLAN: 3 (marketing)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: NONE
Pruning VLANs Enabled: NONE

→ Priority for untagged frames:7
```

How QoS Works

The 2900 XL and 3500 XL switches provide QoS based on IEEE 802.1p class of service (CoS) values.

Typically, networks operate on a *best-effort* delivery basis, which means that all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped.

QoS uses classification and scheduling to transmit network traffic from the switch in a predictable manner. QoS classifies frames by assigning priority-indexed CoS values to them and gives preference to higher-priority traffic.

Note Before you set up QoS-based IEEE 802.1p CoS on a 2900 or 3500 XL switch that operates with the Catalyst 6000 family of switches, refer to the Catalyst 6000 documentation. The Catalyst 6000 switches and the 2900 and 3500 XL switches handle tag information, the ratio of high-priority to low-priority frames, and the buffer queue size differently. You should understand these differences to ensure compatibility.

CoS Values

CoS values range between zero for low-priority and seven for high-priority.

Inter-Switch Link (ISL) frame headers have a 1-byte User field that carries the CoS value in the three least significant bits. IEEE 802.1Q frame headers have a 2-byte Tag Control Information field that carries the 802.1P CoS value in the three most significant bits, which are called the User Priority bits. Other frame types cannot carry CoS values.

Port Priority

Frames received from users in the administratively-defined VLANs are identified or *tagged* for transmission to other devices. Based on rules you define, a unique identifier (the tag) is inserted in each frame header before it is forwarded. The tag is examined and understood by each device before any broadcasts or transmissions to other switches, routers, or end stations. When the frame reaches the last switch or router, the tag is removed before the frame is transmitted to the target end station. VLANs that are assigned on trunk or access ports without identification or a tag are called *native* or *untagged* frames.

Table 2-8 provides information about the types of frames:

Table 2-8 QoS Frame Types

Frame	Description	Tagged?
ISL	Has user priority information specified in the frame header received from the ISL trunk port.	yes
IEEE 802.1Q tagged frames	Has user priority information specified in the frame header received from the 802.1Q trunk port (uses 802.1p).	yes
Untagged frames	No user priority information in the frame header. The port priority is assigned on a VLAN trunk or access port.	no

For ISL or IEEE 802.1Q frames with tag information, the priority value from the header frame is used. For *native* frames, the default priority of the ingress port is used.

Ingress Port Scheduling

Each port on the switch has a single receive queue buffer for incoming traffic. This receive queue buffer is called an *ingress port*. When an untagged frame arrives, it is assigned the value of the port as its port default priority. A tagged frame continues to use its assigned CoS value when it passes through the ingress port.

Egress Port Scheduling

CoS configures each transmit (or *egress*) port with a low-priority transmit queue and a high-priority transmit queue, depending on the frame tag or the port information. See “Transmit Queues” and “Setting the Port Priority for CoS Values” for more information about egress queue priority.

Transmit Queues

As shown in Table 2-9, the switches have two categories of transmit queues:

Table 2-9 Transmit Queue Information

Transmit queue category ¹	Number of transmit queues within each category	Description
2900 XL switches, 2900 XL Ethernet modules (802.1p user priority)	2	Frames with a priority value of 0 through 3 are sent to a normal or low-priority queue. Frames with a priority value of 4 through 7 are sent to a high-priority queue.
3500 XL switches, Gigabit Ethernet modules (802.1p user priority)	2	Frames with a priority value of 0 through 3 are sent to a normal or low-priority queue. Frames with a priority value of 4 through 7 are sent to a high-priority queue.

¹ Legacy switches and modules in this category only have one transmit queue. All frames are sent to a single transmit queue. For a list of devices and corresponding part numbers, see the *Release Notes for Catalyst 2900 Series XL and Catalyst 3500 Series XL Cisco IOS Release 12.0(5)XP*.

Setting the Port Priority for CoS Values

To set the port priority, perform this task in interface configuration mode:

Task	Command
Set port priority on the interface.	switchport priority default <i>default-priority-id</i>

This example shows how to set the port priority:

```
Switch> enable
Switch# password <password>
Switch# configure terminal
Switch(config)# interface fa0/3
Switch(config-if)# switchport priority default 7
Switch(config-if)#
```

Displaying Port Priority Information

To display port priority information, perform this task in user EXEC mode:

Task	Command
Show port priority information for an interface.	show interface <i>interface-id</i> switchport

This example shows how to display the port priority:

```
Switch> show interface fa0/1 switchport  
Name:Fa0/1  
Switchport:Enabled  
Administrative mode:static access  
Operational Mode:static access  
Administrative Trunking Encapsulation:isl  
Operational Trunking Encapsulation:isl  
Negotiation of Trunking:Disabled  
Access Mode VLAN:1 (default)  
Trunking Native Mode VLAN:1 (default)  
Trunking VLANs Enabled:NONE  
Pruning VLANs Enabled:NONE
```

→ Priority for untagged frames:7

