



# CHAPTER 16

## Configuring VLANs, VTP, and VMPS

---

This chapter describes VLANs on Catalyst 4500 series switches. It also describes how to enable the VLAN Trunking Protocol (VTP) and to configure the Catalyst 4500 series switch as a VMPS client.

This chapter includes the following major sections:

- [VLANs, page 16-1](#)
- [VLAN Trunking Protocol, page 16-7](#)
- [VLAN Membership Policy Server, page 16-20](#)



### Note

For complete syntax and usage information for the switch commands used in this chapter, see the *Cisco Catalyst 4500 Series Switch Command Reference* and related publications at this location:

<http://www.cisco.com/en/US/products/hw/switches/ps4324/index.html>

If a command is not in the *Catalyst 4500 Series Switch Command Reference*, you can locate it in the Cisco IOS library. See the *Cisco IOS Command Reference* and related publications at this location:

<http://www.cisco.com/en/US/products/ps6350/index.html>

---

## VLANs

This section includes the following major subsections:

- [About VLANs, page 16-1](#)
- [VLAN Configuration Guidelines and Restrictions, page 16-3](#)
- [VLAN Default Configuration, page 16-4](#)
- [Configuring VLANs, page 16-5](#)

## About VLANs

A VLAN is a group of devices on one or more LANs that are configured to communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

**Note**

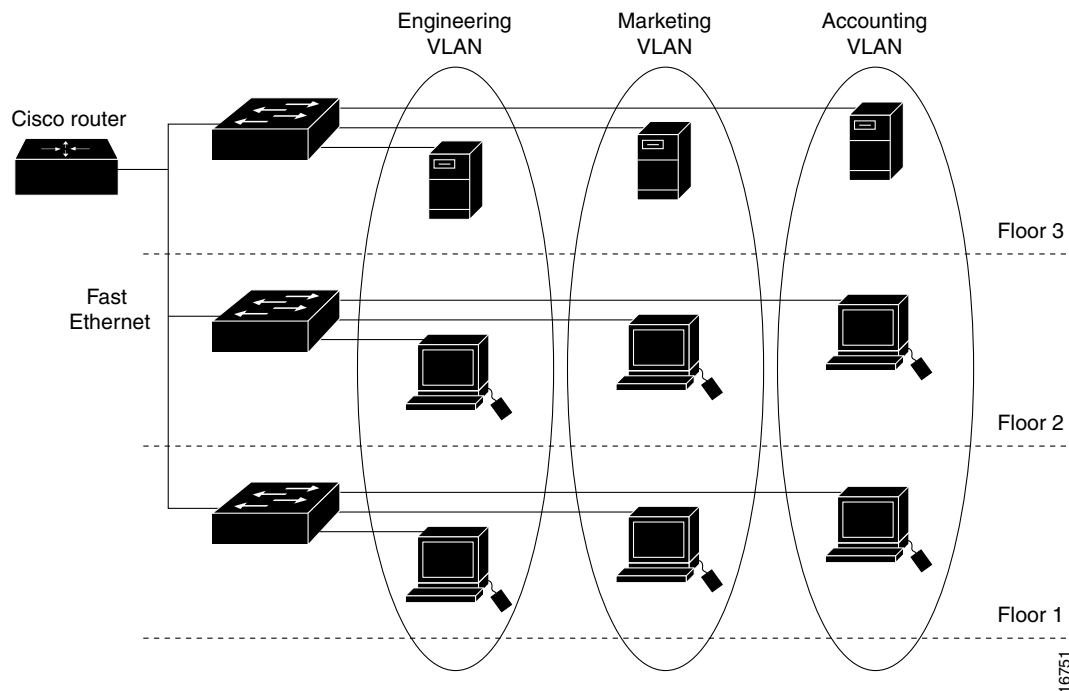
VTP version 3 updates do not pass through promiscuous trunk ports.

VLANs define broadcast domains in a Layer 2 network. A broadcast domain is the set of all devices that receives broadcast frames originating from any device within the set. Broadcast domains are typically bounded by switches because switches do not forward broadcast frames. Layer 2 switches create broadcast domains based on the configuration of the switch. Switches are multiport bridges that allow you to create multiple broadcast domains. Each broadcast domain is like a distinct virtual bridge within a switch.

You can define one or many virtual bridges within a switch. Each virtual bridge you create in the switch defines a new broadcast domain (VLAN). Traffic cannot pass directly to another VLAN (between broadcast domains) within the switch or between two switches. To interconnect two different VLANs, you must use switches or Layer 3 switches. See the “[About Layer 3 Interfaces](#)” section on page 34-1 for information on inter-VLAN routing on Catalyst 4500 series switches.

Figure 16-1 shows an example of three VLANs that create logically defined networks.

**Figure 16-1** Sample VLANs



VLANs are often associated with IP subnetworks. For example, all of the end stations in a particular IP subnet belong to the same VLAN. Traffic between VLANs must be routed. You must assign LAN interface VLAN membership on an interface-by-interface basis (termed interface-based or static VLAN membership).

You can set the following parameters when you create a VLAN in the management domain:

- VLAN number
- VLAN name
- VLAN type

- VLAN state (active or suspended)
- Maximum transmission unit (MTU) for the VLAN
- Security Association Identifier (SAID)
- VLAN number to use when translating from one VLAN type to another

**Note**

---

When the software translates from one VLAN type to another, it requires a different VLAN number for each media type.

---

## VLAN Configuration Guidelines and Restrictions

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

- Before creating a VLAN, put the Catalyst 4500 series switch in VTP server mode or VTP transparent mode. If the Catalyst 4500 series switch is a VTP server, you must define a VTP domain. For information on configuring VTP, see the [“VLAN Trunking Protocol” section on page 16-7](#).
- You cannot use the **end** command in VLAN database mode.
- You cannot use **Ctrl-Z** to exit VLAN database mode.
- If a Catalyst 4948 switch running MSTP and configured with all possible VLANs (4094) is in the path of two HSRP peers with the timeout set below 500 ms, HSRP flaps.

**Workarounds:**

- Use fewer VLANs.
- Set the timers greater than 600 ms.
- Enter the **no igmp snooping** (globally) and **access-list hardware capture mode VLAN** commands

## VLAN Ranges

**Note**

---

You must enable the extended system ID to use 4094 VLANs. See the [“Understanding the Bridge ID” section on page 22-2](#).

---

With Cisco IOS Release 12.2(25)EWA and later, Catalyst 4500 series switches support 4096 VLANs in compliance with the IEEE 802.1Q standard. These VLANs are organized into three ranges: reserved, normal, and extended.

Some of these VLANs are propagated to other switches in the network when you use the VLAN Trunking Protocol (VTP). The extended-range VLANs are not propagated, so you must configure extended-range VLANs manually on each network device.

Table 16-1 describes the uses for VLAN ranges.

**Table 16-1** VLAN Ranges

| VLANs     | Range    | Usage  | Propagated by VTP |
|-----------|----------|--|-------------------|
| 0, 4095   | Reserved | For system use only. You cannot see or use these VLANs.  | —                 |
| 1         | Normal   | Cisco default. You cannot delete this VLAN.  | Yes               |
| 2–1001    | Normal   | Used for Ethernet VLANs; you can create, use, and delete these VLANs.  | Yes               |
| 1002–1005 | Normal   | Cisco defaults for FDDI and Token Ring. You cannot delete VLANs 1002–1005.   | Yes               |
| 1006–4094 | Extended | For Ethernet VLANs only. When configuring extended-range VLANs, note the following: <ul style="list-style-type: none"> <li>• Layer 3 ports and some software features require internal VLANs. Internal VLANs are allocated from 1006 and up. You cannot use a VLAN that has been allocated for such use. To display the VLANs used internally, enter the <b>show vlan internal usage</b> command.</li> <li>• Switches running the Catalyst operating system do not support configuration of VLANs 1006-1024. If you configure VLANs 1006-1024, ensure that the VLANs do not extend to any switches running Catalyst operating system software.</li> <li>• You must enable the extended system ID to use extended range VLANs.</li> </ul> | No                |

## Configurable Normal-Range VLAN Parameters



### Note

Ethernet VLANs 1 and 1006 through 4094 use only default values.

You can configure the following parameters for VLANs 2 through 1001:

- VLAN name
- VLAN type
- VLAN state (active or suspended)
- SAID
- STP type for VLANs

## VLAN Default Configuration

Table 16-2 shows the default VLAN configuration values.

**Table 16-2 Ethernet VLAN Defaults and Ranges**

| Parameter              | Default  | Valid Values              |
|------------------------|--|---------------------------|
| VLAN ID                | 1  | 1–4094                    |
| VLAN name              | VLANx, where x is a number assigned by the software. | No range                  |
| 802.10 SAID            | 100,001  | 1–4,294,967,294           |
| MTU size               | 1500   | 1500–18,190               |
| Translational bridge 1 | 1002   | 0–1005                    |
| Translational bridge 2 | 1003   | 0–1005                    |
| VLAN state             | active   | active; suspend; shutdown |

**Note**

Catalyst 4500 series 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 by using VTP. The software reserves parameters for these media types, but they are not supported.

## Configuring VLANs

**Note**

Before you configure VLANs, you must use VLAN Trunking Protocol (VTP) to maintain global VLAN configuration information for your network. For complete information on VTP, see the [“VLAN Trunking Protocol”](#) section on page 7.

**Note**

VLANs support a number of parameters that are not discussed in detail in this section. For complete information, refer to the *Cisco IOS Command Reference*.

**Note**

The VLAN configuration is stored in the **vlan.dat** file, which is stored in nonvolatile memory. You can cause inconsistency in the VLAN database if you manually delete the **vlan.dat** file. If you want to modify the VLAN configuration or VTP, use the commands described in the following sections and in the *Cisco IOS Command Reference*.

The following sections describe how to configure VLANs:

- [Configuring VLANs in Global Configuration Mode, page 16-6](#)
- [Assigning a Layer 2 LAN Interface to a VLAN, page 16-7](#)

## Configuring VLANs in Global Configuration Mode

If the switch is in VTP server or transparent mode (see the “[VLAN Trunking Protocol](#)” section on [page 16-7](#)), you can configure VLANs in global and VLAN configuration modes. When you configure VLANs in global and config-vlan configuration modes, the VLAN configuration is saved in the **vlan.dat** files, not the **running-config** or **startup-config** files. To display the VLAN configuration, enter the **show vlan** command.

If the switch is in VLAN transparent mode, use the **copy running-config startup-config** command to save the VLAN configuration to the **startup-config** file. After you save the running configuration as the startup configuration, the **show running-config** and **show startup-config** commands display the VLAN configuration.



### Note

When the switch boots, if the VTP domain name and VTP mode in the **startup-config** and **vlan.dat** files do not match, the switch uses the configuration in the **vlan.dat** file.

You use the interface configuration command mode to define the port membership mode and add and remove ports from a VLAN. The results of these commands are written to the **running-config** file, and you can display the contents of the file by entering the **show running-config** command. Beginning with Cisco IOS Release 15.2(2)E and Cisco IOS XE Release 3.6E, if the VTP mode is off or transparent, VLAN configuration is saved to the **startup-config** file, even when the configuration is not applied to the interface.

User-configured VLANs have unique IDs from 1 to 4094. To create a VLAN, enter the **vlan** command with an unused ID. To verify whether a particular ID is in use, enter the **show vlan id ID** command. To modify a VLAN, enter the **vlan** command for an existing VLAN.

See the “[VLAN Default Configuration](#)” section on [page 16-4](#) for the list of default parameters that are assigned when you create a VLAN. If you do not use the **media** keyword when specifying the VLAN type, the VLAN is an Ethernet VLAN.

To create a VLAN, perform this task:

|        | Command  | Purpose  |
|--------|--|--|
| Step 1 | Switch# <b>configure terminal</b>  | Enters global configuration mode.  |
| Step 2 | Switch(config)# <b>vlan</b> <i>vlan_ID</i><br>Switch(config-vlan)#       | Adds an Ethernet VLAN.<br><br><b>Note</b> You cannot delete the default VLANs for these media types: Ethernet VLAN 1 and FDDI or Token Ring VLANs 1002 to 1005.<br>When you delete a VLAN, any LAN interfaces configured as access ports assigned to that VLAN become inactive. They remain associated with the VLAN (and thus inactive) until you assign them to a new VLAN.<br><br>Use the <b>no</b> keyword to delete a VLAN.<br><br>When the prompt shows <b>Switch(config-vlan)#</b> ; you are in vlan-configuration mode. If you want to change any of the parameters for the newly created VLAN, use this mode. |
| Step 3 | Switch(config-vlan)# <b>end</b>  | Returns to enable mode from vlan-configuration mode.   |
| Step 4 | Switch# <b>show vlan</b> [ <i>id</i>   <i>name</i> ]<br><i>vlan_name</i> | Verifies the VLAN configuration.   |

When you create or modify an Ethernet VLAN, note the following:

- Because Layer 3 ports and some software features require internal VLANs allocated from 1006 and up, configure extended-range VLANs starting with 4094 and work downward.
- You can configure extended-range VLANs only in global configuration mode. You cannot configure extended-range VLANs in VLAN database mode.
- Layer 3 ports and some software features use extended-range VLANs. If the VLAN you are trying to create or modify is being used by a Layer 3 port or a software feature, the switch displays a message and does not modify the VLAN configuration.
- When you create VLANs with the VLAN configuration command, they are automatically added to the existing VTP domain; no action is required of the user.

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

```
Switch# configure terminal
Switch(config)# vlan 3
Switch(config-vlan)# end
Switch# show vlan id 3
```

| VLAN Name  | Status     | Ports |
|--|------------|-------|
| 3 VLAN0003   | active     |       |
| VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2 |            |       |
| 3 enet 100003 1500 - - - - - 0 0                                     |            |       |
| Primary Secondary Type   | Interfaces |       |

```
Switch#
```

## Assigning a Layer 2 LAN Interface to a VLAN

A VLAN created in a management domain remains unused until you assign one or more LAN interfaces to the VLAN.



### Note

Make sure you assign LAN interfaces to a VLAN of the proper type. Assign Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet interfaces to Ethernet-type VLANs.

To assign one or more LAN interfaces to a VLAN, complete the procedures in the [“Configuring Ethernet Interfaces for Layer 2 Switching”](#) section on page 18-5.

## VLAN Trunking Protocol

This section describes the VLAN Trunking Protocol (VTP) on the Catalyst 4500 series switches, and includes the following major subsections:

- [About VTP, page 16-8](#)
- [VTP Configuration Guidelines and Restrictions, page 16-12](#)
- [VTP Default Configuration, page 16-13](#)
- [Configuring VTP, page 16-14](#)

## About VTP

VTP is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs within a VTP domain. A VTP domain (also called a VLAN management domain) is made up of one or more network devices that share the same VTP domain name and that are interconnected with trunks. VTP minimizes misconfigurations and configuration inconsistencies that can result in a number of problems, such as duplicate VLAN names, incorrect VLAN-type specifications, and security violations.

Before you create VLANs, you must decide whether you want to use VTP in your network. With VTP, you can make configuration changes centrally on one or more network devices and have those changes automatically communicated to all the other network devices in the network. For details on configuring VLANs, see the “VLANs” section on page 16-1

These sections describe how VTP works:

- [Understanding the VTP Domain, page 16-8](#)
- [Understanding VTP Modes, page 16-9](#)
- [Understanding VTP Advertisements, page 16-9](#)
- [Understanding VTP Versions, page 16-9](#)
- [Understanding VTP Pruning, page 16-11](#)

## Understanding the VTP Domain

A VTP domain is made up of one or more interconnected network devices that share the same VTP domain name. A network device can be configured to be in only one VTP domain. You make global VLAN configuration changes for the domain using either the command-line interface (CLI) or Simple Network Management Protocol (SNMP).

By default, the Catalyst 4500 series switch is in VTP server mode and the domain is set to NULL until the switch receives an advertisement for a domain over a trunk link or you configure a management domain. You cannot create or modify VLANs on a VTP server until the 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 the VTP configuration revision number. The switch ignores advertisements with a different management domain name or an earlier configuration revision number.

If you configure the switch as VTP transparent, you can create and modify VLANs, but the changes affect only the individual switch.

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

VTP maps VLANs dynamically across multiple LAN types with unique names and internal index associations. Mapping eliminates unnecessary device administration for network administrators.



## Understanding VTP Modes

You can configure a Catalyst 4500 series switch to operate in any one of these VTP modes:

- **Server**—In VTP server mode, you can create, modify, and delete VLANs and specify other configuration parameters (such as VTP version and VTP pruning) for the entire VTP domain. VTP servers advertise their VLAN configuration to other network devices in the same VTP domain and synchronize their VLAN configuration with other network devices based on advertisements received over trunk links. VTP server is the default mode.



---

**Note** In VTP version 3, manipulation of VLANs can be done only to primary servers.

---

- **Client**—VTP clients behave the same way as VTP servers, but you cannot create, change, or delete VLANs on a VTP client.
- **Transparent**—VTP transparent network devices do not participate in VTP. A VTP transparent network device does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. However, in VTP version 2, transparent network devices do forward VTP advertisements that they receive on their trunking LAN interfaces.
- **Off**—In VTP off mode, a network device functions in the same manner as a VTP transparent device except that it does not forward VTP advertisements.



**Note**

---

Catalyst 4500 series switches automatically change from VTP server mode to VTP client mode if the switch detects a failure while writing configuration to NVRAM. If this happens, the switch cannot be returned to VTP server mode until the NVRAM is functioning.

---

## Understanding VTP Advertisements

Each network device in the VTP domain sends periodic advertisements out each trunking LAN interface to a reserved multicast address. VTP advertisements are received by neighboring network devices, which update their VTP and VLAN configurations as necessary.

The following global configuration information is distributed in VTP advertisements:

- VLAN IDs (ISL and 802.1Q)
- Emulated LAN names (for ATM LANE)
- 802.10 SAID values (FDDI)
- VTP domain name
- VTP configuration revision number
- VLAN configuration, including maximum transmission unit (MTU) size for each VLAN
- Frame format

## Understanding VTP Versions

### VTP Version 2

If you use VTP in your network, you must decide whether to use VTP version 2 or version 3.

**Note**

Catalyst 4500 series switches do not support Token Ring or FDDI media. The switch does not forward FDDI, FDDI-Net, Token Ring Concentrator Relay Function (TrCRF), or Token Ring Bridge Relay Function (TrBRF) traffic, but it does propagate the VLAN configuration by using VTP.

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

- Token Ring support—Supports Token Ring LAN switching and VLANs (TrBRF and TrCRF).
- 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.
- Version-dependent transparent mode—In VTP version 1 and version 2, a VTP transparent network device forwards VTP messages in transparent mode without checking the version.
- 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 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 digest on a received VTP message is correct, its information is accepted without consistency checks.

**VTP Version 3**

VTP version 3 supports the following features not supported in version 1 or version 2:

- Hidden password support—Supports the option of configuring the password as **hidden** or **secret**.  
When the **hidden** keyword is specified, that password must be reentered if a takeover command is issued in the domain. The secret key generated from the password string is saved in the `const_nvram:vlan.dat` file. When configured with this option, the password does not appear in plain text in the configuration. Instead, the secret key associated with the password is saved in hexadecimal format in the running configuration. If the **hidden** keyword is not specified, the password is saved in clear text in the `const_nvram:vlan.dat` file as in VTP version 1 and VTP version 2.  
When the **secret** keyword is specified, the password secret key can be directly configured.
- Extended VLAN database propagation support—In VTP version 2, VLAN configuration information is propagated only for VLANs numbered 1 to 1000. In VTP version 3, information also is propagated for extended-range VLANs (VLANs numbered 1006 to 4094).
- On Catalyst 4500 series switches running VTP version 1, VTP version 2, or VTP version 3, default VLANs 1 and 1002 to 1005 cannot be modified.

**Note**

VTP pruning continues to apply only to VLANs numbered 1 to 1000.

- Propagation of any database in a domain—In addition to propagating VLAN database information, VTP can propagate Multiple Spanning Tree (MST) protocol database information.
- Disabling VTP—When VTP is disabled on a trunking port, it applies to all VTP instances on that port. When VTP is disabled globally, the setting applies to all the trunking ports in the system.
- In VTP version 1 and VTP version 2, the role of a VTP server is to back up the database to NVRAM and to allow the administrator to change database information. VTP version 3 introduces the roles of VTP primary server and VTP secondary server. A VTP primary server is used to update the

database information. The updates sent out are honored by all the devices in the system. A VTP secondary server can only back up to its NVRAM the VTP configuration received by using updates from the VTP primary server.

The status of primary and secondary servers is a runtime status and is not a configurable option. By default, all devices are initiated as secondary servers. Primary server status is needed only when database updates are needed, and is obtained when the administrator issues a takeover message in the domain. See the [“Starting a Takeover” section on page 16-19](#).

Primary server status is lost upon reload of the device, or when switchover or domain parameters change. Secondary servers back up the configuration and continue to propagate it. Because of that, you may have a working VTP domain without any primary servers.

## Understanding VTP Pruning

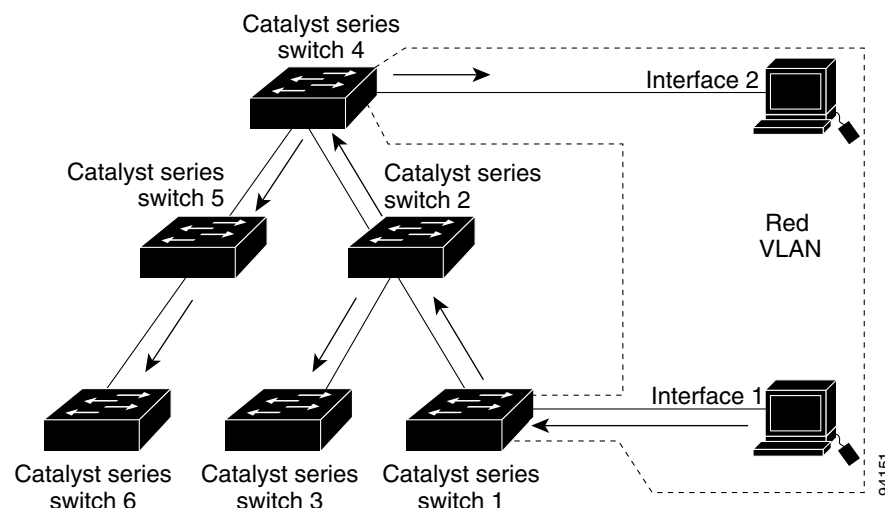
VTP pruning enhances network bandwidth use by reducing unnecessary flooded traffic, such as broadcast, multicast, and unicast packets. VTP pruning increases available bandwidth by restricting flooded traffic to those trunk links that the traffic must use to access the appropriate network devices. By default, VTP pruning is disabled.

For VTP pruning to be effective, all devices in the management domain must either support VTP pruning or, on devices that do not support VTP pruning, you must manually configure the VLANs allowed on trunks.

[Figure 16-2](#) shows a switched network without VTP pruning enabled. Interface 1 on Switch 1 and Interface 2 on Switch 4 are assigned to the Red VLAN. A broadcast is sent from the host connected to Switch 1. Switch 1 floods the broadcast and every network device in the network receives it, even though Switches 3, 5, and 6 have no interfaces in the Red VLAN.

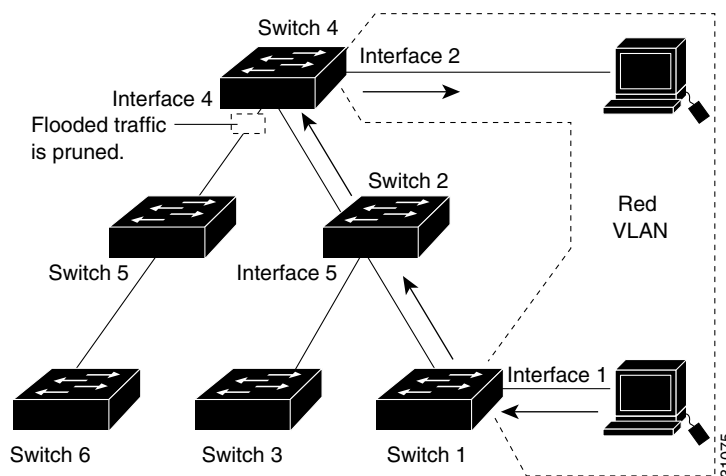
You can enable pruning globally on the Catalyst 4500 series switch (see the [“Enabling VTP Pruning” section on page 16-15](#)).

**Figure 16-2 Flooding Traffic without VTP Pruning**



[Figure 16-3](#) shows the same 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 indicated (Interface 5 on Switch 2 and Interface 4 on Switch 4).

Figure 16-3 Flooding Traffic with VTP Pruning



Enabling VTP pruning on a VTP server enables pruning for the entire management domain. VTP pruning takes effect several seconds after you enable it. By default, VLANs 2 through 1000 are eligible for pruning. VTP pruning does not prune traffic from pruning-ineligible VLANs. VLAN 1 is always ineligible for pruning; traffic from VLAN 1 cannot be pruned.

To configure VTP pruning on a trunking LAN interface, use the **switchport trunk pruning vlan** command. VTP pruning operates when a LAN interface is trunking. You can set VLAN pruning eligibility regardless of whether VTP pruning is enabled or disabled for the VTP domain, whether any given VLAN exists, and regardless of whether the LAN interface is currently trunking.

## VTP Configuration Guidelines and Restrictions

Follow these guidelines and restrictions when implementing VTP in your network:

- Supervisor engine redundancy does not support nondefault VLAN data file names or locations. Do not enter the **vtp file file\_name** command on a switch that has a redundant supervisor engine.
- Before installing a redundant supervisor engine, enter the **no vtp file** command to return to the default configuration.
- When a VTP version 3 device on a trunk port receives messages from a VTP version 2 device, it sends a scaled-down version of the VLAN database on that particular trunk in a VTP version 2 format. A VTP version 3 device does not send out VTP version 2 formatted packets on a trunk port unless it first receives VTP version 2 packets on that trunk.
- Even when a VTP version 3 device detects a VTP version 2 device on a trunk port, it continues to send VTP version 3 packets in addition to VTP version 2 packets, to allow co-existence of two kinds of neighbors off the trunk.
- A VTP version 3 device does not accept configuration information from a VPT version 2 or version 1 device.
- Unlike in VPT version 2, when VTP is configured to be version 3, this does not configure all the version-3-capable devices in the domain to start behaving as VPT version 3 systems.
- When a VTP version 1 device, capable of version 2 or version 3, receives a VTP version 3 packet, the device is configured as a VTP version 2 device provided a VTP version 2 conflict does not exist.
- Devices that are only VTP version 1 capable cannot interoperate with VTP version 3 devices.

- In a Token Ring environment, you must enable VTP version 2 or version 3 for Token Ring VLAN switching to function properly.
- Two VTP version 3 regions can only communicate in transparent mode over a VTP version 1 or VTP version 2 region.
- All network devices in a VTP domain must run the same VTP version.
- You must configure a password on each network device in the management domain when VTP is in secure mode.

**Caution**

If you configure VTP in secure mode and you do not assign a management domain password to each network device in the domain, the management domain does not function properly.

- A VTP version 2-capable network device can operate in the same VTP domain as a network device running VTP version 1 if VTP version 2 is disabled on the VTP version 2-capable network device (VTP version 2 is disabled by default).
- Do not enable VTP version 2 on a network device unless all of the network devices in the same VTP domain are version 2-capable. When you enable VTP version 2 on a server, all of the version 2-capable network devices in the domain enable VTP version 2.
- Enabling or disabling VTP pruning on a VTP server enables or disables VTP pruning for the entire management domain.
- Configuring VLANs as eligible for pruning on a Catalyst 4500 series switch affects pruning eligibility for those VLANs on that switch only, not on all network devices in the VTP domain.
- The VLAN database is saved in the NVRAM file in a format compliant with the VTP version running on the system. Since older images supporting only VTP version 2 do not recognize the VTP version 3 file format, the NVRAM VLAN database information is lost if the system is downgraded from a new image supporting VTP to one that does not.

## VTP Default Configuration

Table 16-3 shows the default VTP configuration.

**Table 16-3 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              |

The default VTP mode for newly manufactured Catalyst 4500 supervisor engines, Catalyst 4900 series switches, and the Cisco ME 4924-10GE switch is transparent. Deleting `vlan.dat` or entering the `erase cat4000_flash:` command, and resetting the switch changes the VTP mode to server.

## Configuring VTP

These sections describe how to configure VTP:

- [Configuring VTP Global Parameters, page 16-14](#)
- [Configuring the VTP Mode, page 16-16](#)
- [Starting a Takeover, page 16-19](#)
- [Displaying VTP Statistics, page 16-19](#)
- [Displaying VTP Devices in a Domain, page 16-20](#)

## Configuring VTP Global Parameters

These sections describe configuring the VTP global parameters:

- [Configuring a VTP Password, page 16-14](#)
- [Enabling VTP Pruning, page 16-15](#)
- [Enabling the VTP Version Number, page 16-15](#)



### Note

You can enter the VTP global parameters in either global configuration mode or in EXEC mode.

## Configuring a VTP Password

To configure the VTP global parameters, use these commands:

| Command   | Purpose   |
|---|---|
| Switch(config)# <b>vtp password</b><br><i>password_string</i> [ <b>hidden</b>   <b>secret</b> ] | Sets a password, which can be from 8 to 64 characters long, for the VTP domain.<br><br>In VTP version 3 the keywords <b>hidden</b> and <b>secret</b> are available. <ul style="list-style-type: none"> <li>• If the <b>hidden</b> keyword is used, the secret key generated from the password string is saved in the <code>const_nvram:vlan.dat</code> file. If a takeover command is issued, that password must be reentered.</li> <li>• If the <b>secret</b> keyword is used, the password secret key can be directly configured. The <b>secret</b> password must contain 32 hexadecimal characters.</li> </ul> |
| Switch(config)# <b>no vtp password</b>  | Clears the password.  |

This example shows one way to configure a VTP password in global configuration mode:

```
Switch# configure terminal
Switch(config)# vtp password WATER
Setting device VLAN database password to WATER.
Switch#
```

This example shows how to configure a VTP password in EXEC mode:

```
Switch# vtp password WATER
Setting device VLAN database password to WATER.
Switch#
```

**Note**

The password is not stored in the running-config file.

This example shows how to configure a **hidden** password:

```
Switch# configure terminal
Switch(config)# vtp password WATER hidden
Generating the secret associated to the password.
Switch(config)#
```

This example shows how the password WATER is displayed when it is configured with the **hidden** keyword.

```
Switch# show vtp password
VTP Password: 89914640C8D90868B6A0D8103847A733
Switch#
```

## Enabling VTP Pruning

To enable VTP pruning in the management domain, perform this task:

|        | Command  | Purpose                                       |
|--------|--|---|
| Step 1 | Switch(config)# <b>vtp pruning</b>               | Enables VTP pruning in the management domain. |
| Step 2 | Switch# <b>show vtp status   include pruning</b> | (Optional) Verifies the configuration.        |

This example shows one way to enable VTP pruning in the management domain:

```
Switch# configure terminal
Switch(config)# vtp pruning
Pruning switched ON
```

This example shows how to enable VTP pruning in the management domain with any release:

```
Switch# vtp pruning
Pruning switched ON
```

This example shows how to verify the configuration:

```
Switch# show vtp status | include Pruning
VTP Pruning Mode: Enabled
Switch#
```

For information about configuring prune eligibility, see the [“Understanding VTP Pruning” section on page 16-11](#).

## Enabling the VTP Version Number

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

**Caution**

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

**Note**

In a Token Ring environment, you must enable VTP version 2 or VTP version 3 for Token Ring VLAN switching to function properly on devices that support Token Ring interfaces.

To enable the VTP version, perform this task:

|        | Command  | Purpose                                |
|--------|--|--|
| Step 1 | Switch(config)# <b>vtp version</b> {1   2   3}                 | Enables the VTP version.               |
| Step 2 | Switch# <b>show vtp status</b>   <b>include</b> {v1   v2   v3} | (Optional) Verifies the configuration. |

This example shows one way to enable VTP version 2:

```
Switch# configure terminal
Switch(config)# vtp version 2
V2 mode enabled.
Switch(config)#
```

This example shows how to enable VTP version 2 with any release:

```
Switch# vtp version 2
V2 mode enabled.
Switch#
```

This example shows how to verify the configuration:

```
Switch# show vtp status | include v2
VTP V2 Mode: Enabled
Switch#
```

## Configuring the VTP Mode

To configure the VTP mode, perform this task:

|        | Command   | Purpose  |
|--------|---|--|
| Step 1 | Switch(config)# <b>vtp mode</b> {client   server   transparent   off} | Configures the VTP mode.   |
| Step 2 | Switch(config)# <b>vtp domain</b> <i>domain_name</i>                  | (Optional; for server mode only) Defines the VTP domain name, which can be up to 32 characters long. VTP server mode requires a domain name. If the switch has a trunk connection to a VTP domain, the switch learns the domain name from the VTP server in the domain.<br><b>Note</b> You cannot clear the domain name. |
| Step 3 | Switch(config)# <b>end</b>  | Exits VLAN configuration mode.   |
| Step 4 | Switch# <b>show vtp status</b>  | (Optional) Verifies the configuration.   |



**Note**

When VTP is disabled, you can enter VLAN configuration commands in configuration mode instead of the VLAN database mode and the VLAN configuration is stored in the startup configuration file.

This example shows how to configure the switch as a VTP server:

```
Switch# configure terminal
Switch(config)# vtp mode server
Setting device to VTP SERVER mode.
Switch(config)# vtp domain Lab_Network
Setting VTP domain name to Lab_Network
Switch(config)# end
Switch#
```

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

```
Switch# configure terminal
Switch(config)# vtp mode client
Setting device to VTP CLIENT mode.
Switch(config)# end
Switch#
```

This example shows how to disable VTP on the switch:

```
Switch# configure terminal
Switch(config)# vtp mode transparent
Setting device to VTP TRANSPARENT mode.
Switch(config)# end
Switch#
```

This example shows how to disable VTP on the switch and to disable VTP advertisement forwarding:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# vtp mode off
Setting device to VTP OFF mode.
Switch(config)# end
Switch#
```

This example shows an example of the VTP configuration parameters when the device is running VTP version 1:

```
Switch# show vtp status
VTP Version capable          : 1 to 3
VTP version running         : 1
VTP Domain Name             : Lab_Network
VTP Pruning Mode            : Enabled
VTP Traps Generation        : Disabled
Device ID                   : 0016.9c6d.5300
Configuration last modified by 127.0.0.12 at 10-18-07 10:12:42
Local updater ID is 127.00.12 at 10-18-07 10:2:42

Feature VLAN:
-----
VTP Operating Mode          : Server
Maximum number of existing VLANs : 5
Configuration Revision      : 1
MD5 digest                  : 0x92 0xF1 0xE8 0x52 0x2E 0x5C 0x36 0x10 0x70 0x61 0xB8
                             0x24 0xB6 0x93 0x21 0x09

Switch#
```

This example shows an example of the VTP configuration parameters when the device is running VTP version 2:

```
Switch# show vtp status
VTP Version capable      : 1 to 3
VTP version running     : 2
VTP Domain Name         : Lab_Network
VTP Pruning Mode        : Disabled
VTP Traps Generation    : Disabled
Device ID                : 0012.44dc.b800
Configuration 1st modified by 127.0.0.12 at 10-18-07 10:38:45
Local updater ID is 127.0.0.12 on interface EO 0/0 (first interface found)
```

Feature VLAN:

```
-----
VTP Operating Mode      : Server
Maximum VLANs supported locally: 1005
Number of existing VLANs : 1005
Configuration Revision  : 1
MD5 digest              : 0x2E 0x6B 0x99 0x58 0xA2 0x4F 0xD5 0x150x70 0x61 0xB8
                        0x24 0xB6 0x93 0x21 0x09
```

Switch#

This example shows an example of the VTP configuration parameters when the device is running VTP version 3:

```
Switch# show vtp status
VTP Version capable      : 1 to 3
VTP version running     : 3
VTP Domain Name         : Lab_Network
VTP Pruning Mode        : Disabled
VTP Traps Generation    : Disabled
Device ID                : 0012.44dc.b800
```

Feature VLAN:

```
-----
VTP Operating Mode      : Server
Number of existing VLANs : 1005
Number of existing extended VLANs: 3074
Configuration Revision  : 18
Primary ID              : 0012.4371.9ec0
Primary Description     :
Switch#
```

## Starting a Takeover

This process applies to VTP version 3 only. To start a takeover, perform this task:

| Command  | Purpose   |
|--|---|
| Switch# <b>vtp primary-server</b> [vlan   mst]   [force] | <p>Changes the operational state of a switch from a secondary to a primary server and advertises the configuration to the whole domain. (If the password for this device is configured with the <b>hidden</b> keyword, the user is prompted to re-enter it.)</p> <p><b>Note</b> Using the <b>force</b> keyword overwrites the configuration of any conflicting servers. If not using the <b>force</b> keyword, you are prompted for confirmation before proceeding with the takeover.</p> <p>Specify where to direct the takeover by selecting the appropriate feature (<b>vlan</b> or <b>mst</b>). If no feature is selected, the takeover is directed to the VLAN database.</p> |

This example shows how to start a takeover and direct it to the **vlan** database:

```
Switch# vtp primary-server vlan
Enter VTP password:password
This system is becoming primary for feature vlan

VTP Feature Conf Revision Primary Server Device ID      Description
-----
MST          Yes    4           0012.4371.9ec0=0012.4371.9ec0 R1
Do you want to continue? (confirm)
Switch#
```

## Displaying VTP Statistics

To display VTP statistics, including VTP advertisements sent and received and VTP errors, perform this task:

| Command                          | Purpose                  |
|----------------------------------|--------------------------|
| Switch# <b>show vtp counters</b> | Displays VTP statistics. |

This example shows how to display VTP statistics:

```
Switch# show vtp counters
VTP statistics:
Summary advertisements received      : 7
Subset advertisements received      : 5
Request advertisements received     : 0
Summary advertisements transmitted  : 997
Subset advertisements transmitted   : 13
Request advertisements transmitted   : 3
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 |
|-------|------------------|---------------|--|
| ----- | -----            | -----         | -----  |
| Fa5/8 | 43071            | 42766         | 5  |

## Displaying VTP Devices in a Domain

To display information for all the VTP devices in a domain, perform this task:

| Command  | Purpose  |
|--|--|
| Switch# <b>show vtp devices</b> [ <b>conflicts</b> ] | <p>Gathers and displays information for all the VTP devices in the domain.</p> <p><b>Note</b> No information is gathered or displayed from switches set to <b>vtp modes off</b> or to <b>transparent</b> for a particular feature.</p> <p>The <b>conflicts</b> keyword (optional) displays the information of devices that have conflicting primary servers.</p> |

This example shows how to display information for VTP devices in a domain:

```
Switch# show vtp devices
Retrieving information from the VTP domain, please wait for 5 seconds.
VTP Feature Conf Revision Primary Server Device ID      Device Description
-----
VLAN          No   18      0016.9c6d.5300 0012.011a.0d00   R2
VLAN          No   18      0016.9c6d.5300 0012.4371.9ec0   R1
MST           Yes   4       0012.4371.9ec0=0012.4371.9ec0 R1

Switch#
```

## VLAN Membership Policy Server

This section describes how to configure dynamic port VLAN membership through the VLAN Membership Policy Server (VMPS), and includes the following subsections:

- [About VMPS, page 16-20](#)
- [Overview of VMPS Clients, page 16-23](#)
- [Dynamic Port VLAN Membership Configuration Example, page 16-29](#)
- [VMPS Database Configuration File Example, page 16-32](#)

## About VMPS

These subsections describe what a VMPS server does and how it operates:

- [Understanding the VMPS Server, page 16-21](#)
- [Security Modes for VMPS Server, page 16-21](#)

- [Fallback VLAN, page 16-22](#)
- [Illegal VMPS Client Requests, page 16-23](#)

## Understanding the VMPS Server

A VLAN Membership Policy Server (VMPS) provides a centralized server for selecting the VLAN for a port dynamically based on the MAC address of the device connected to the port. When the host moves from a port on one switch in the network to a port on another switch in the network, that switch dynamically assigns the new port to the proper VLAN for that host.

A Catalyst 4500 series switch running Cisco IOS software does not support the functionality of a VMPS. It can only function as a VLAN Query Protocol (VQP) client, which communicates with a VMPS through the VQP. For VMPS functionality, you need to use a Catalyst 4500 series switch (or Catalyst 6500 series switch) running Catalyst operating system (OS) software.

VMPS uses a UDP port to listen to VQP requests from clients, so, it is not necessary for VMPS clients to know if the VMPS resides on a local or remote device on the network. Upon receiving a valid request from a VMPS client, a VMPS server searches its database for an entry of a MAC-address to VLAN mapping.

In response to a request, the VMPS takes one of the following 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” (open), a “fallback VLAN name” (open with fallback VLAN configured), a “port-shutdown” (secure), or a “new VLAN name” (multiple) response, depending on the secure mode setting of the VMPS.

If the switch receives an “access-denied” response from the VMPS, the switch 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, the switch disables the port. The port must be manually reenabled by using the CLI, Cisco Visual Switch Manager (CVSM), 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.

## Security Modes for VMPS Server

VMPS operates in three different modes. The way a VMPS server responds to illegal requests depends on the mode in which the VMPS is configured:

- [Open Mode, page 16-22](#)
- [Secure Mode, page 16-22](#)
- [Multiple Mode, page 16-22](#)

## Open Mode

If no VLAN is assigned to this port, VMPS verifies the requesting MAC address against this port:

- If the VLAN associated with this MAC address is allowed on the port, the VLAN name is returned to the client.
- If the VLAN associated with this MAC address is not allowed on the port, the host receives an “access denied” response.

If a VLAN is already assigned to this port, VMPS verifies the requesting MAC address against this port:

- If the VLAN associated with this MAC address in the database does not match the current VLAN assigned on the port, and a fallback VLAN name is configured, VMPS sends the fallback VLAN name to the client.
- If a VLAN associated with this MAC address in the database does not match the current VLAN assigned on the port, and a fallback VLAN name is not configured, the host receives an “access denied” response.

## Secure Mode

If no VLAN is assigned to this port, VMPS verifies the requesting MAC address against this port:

- If the VLAN associated with this MAC address is allowed on the port, the VLAN name is returned to the client.
- If the VLAN associated with this MAC address is not allowed on the port, the port is shut down.

If a VLAN is already assigned to this port, VMPS verifies the requesting MAC address against this port:

- If a VLAN associated with this MAC address in the database does not match the current VLAN assigned on the port, the port is shutdown, even if a fallback VLAN name is configured.

## Multiple Mode

Multiple hosts (MAC addresses) can be active on a dynamic port if they are all in the same VLAN. If the link fails on a dynamic port, the port returns to the unassigned state. Any hosts that come online through the port are checked again with VMPS before the port is assigned to a VLAN.

If multiple hosts connected to a dynamic port belong to different VLANs, the VLAN matching the MAC address in the last request is returned to the client provided that multiple mode is configured on the VMPS server.



### Note

Although Catalyst 4500 series and Catalyst 6500 series switches running Catalyst operating system software support VMPS in all three operation modes, the User Registration Tool (URT) supports open mode only.

## Fallback VLAN

You can configure a fallback VLAN name on a VMPS server.

If no VLAN has been assigned to this port, VMPS compares the requesting MAC address to this port:

- 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 name and the MAC address does not exist in the database, the VMPS sends an “access-denied” response.

If a VLAN is already assigned to this port, VMPS compares the requesting MAC address to this port:

- If the VMPS is in secure mode, it sends a “port-shutdown” response, whether a fallback VLAN has been configured on the server.

## Illegal VMPS Client Requests

Two examples of illegal VMPS client requests are as follows:

- When a MAC-address mapping is not present in the VMPS database and “no fall back” VLAN is configured on the VMPS.
- When a port is already assigned a VLAN (and the VMPS mode is not “multiple”) but a second VMPS client request is received on the VMPS for a different MAC-address.

## Overview of VMPS Clients

The following subsections describe how to configure a switch as a VMPS client and configure its ports for dynamic VLAN membership.

The following topics are included:

- [Understanding Dynamic VLAN Membership, page 16-23](#)
- [Default VMPS Client Configuration, page 16-24](#)
- [Configuring a Switch as a VMPS Client, page 16-24](#)
- [Administering and Monitoring the VMPS, page 16-27](#)
- [Troubleshooting Dynamic Port VLAN Membership, page 16-28](#)

## Understanding Dynamic VLAN Membership

When a port is configured as “dynamic,” it receives VLAN information based on the MAC-address that is on the port. The VLAN is not statically assigned to the port; it is dynamically acquired from the VMPS based on the MAC-address on the port.

A dynamic port can belong to one VLAN only. When the link becomes active, the switch does not forward traffic to or from this port until the port is assigned to a VLAN. The source MAC address from the first packet of a new host on the dynamic port is sent to the VMPS as part of the VQP request, which 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 there is no match, the VMPS either denies the request or shuts down the port (depending on the VMPS security mode setting). See the “[About VMPS](#)” section on [page 16-20](#) for a complete description of possible VMPS responses.

Multiple hosts (MAC addresses) can be active on a dynamic port if all are in the same VLAN. If the link goes down on a dynamic port, the port returns to the unassigned state and does not belong to a VLAN. Any hosts that come online through the port are checked again with the VMPS before the port is assigned to a VLAN.

For this operation to work, the client device must be able to reach the VMPS. A VMPS client sends VQP requests as UDP packets, trying a certain number of times before giving up. For details on how to set the retry interval, refer to section “[Configuring the Retry Interval](#)” on [page 27](#).

The VMPS client also periodically reconfirms the VLAN membership. For details on how to set the reconfirm frequency, refer to section “[Administering and Monitoring the VMPS](#)” on [page 27](#).

A maximum of 50 hosts are supported on a given port at any given time. Once this maximum is exceeded, the port is shut down, irrespective of the operating mode of the VMPS server.

**Note**

The VMPS shuts down a dynamic port if more than 50 hosts are active on that port.

## Default VMPS Client Configuration

Table 16-4 shows the default VMPS and dynamic port configuration on client switches.

**Table 16-4** Default VMPS Client and Dynamic Port Configuration

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

## Configuring a Switch as a VMPS Client

This section contains the following topics:

- [Configuring the IP Address of the VMPS Server, page 16-24](#)
- [Configuring Dynamic Access Ports on a VMPS Client, page 16-25](#)
- [Reconfirming VLAN Memberships, page 16-26](#)
- [Configuring Reconfirmation Interval, page 16-26](#)
- [Reconfirming VLAN Memberships, page 16-26](#)

## Configuring the IP Address of the VMPS Server

To configure a Catalyst 4500 series switch as a VMPS client, you must enter the IP address or hostname of the switch acting as the VMPS.

To define the primary and secondary VMPS on a Catalyst 4500 series switch, perform this task:

|               | Command  | Purpose   |
|---------------|--|---|
| <b>Step 1</b> | Switch# <b>configure terminal</b>  | Enters global configuration mode.   |
| <b>Step 2</b> | Switch(config)# <b>vmips server</b><br>{ <i>ipaddress</i>   <i>hostname</i> } <b>primary</b> | Specifies the IP address or hostname of the switch acting as the primary VMPS server. |
| <b>Step 3</b> | Switch(config)# <b>vmips server</b><br>{ <i>ipaddress</i>   <i>hostname</i> }                | Specifies the IP address or hostname of the switch acting as a secondary VMPS server. |
| <b>Step 4</b> | Switch(config)# <b>end</b>   | Returns to privileged EXEC mode.  |
| <b>Step 5</b> | Switch# <b>show vmips</b>  | Verifies the VMPS server entry.   |

This example shows how to define the primary and secondary VMPS devices:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```



```
Switch(config)# vmps server 172.20.128.179 primary
Switch(config)# vmps server 172.20.128.178
Switch(config)# end
```

**Note**

You can configure up to four VMPS servers using this CLI on the VMPS client.

```
Switch# show vmps
VQP Client Status:
-----
VMPS VQP Version: 1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server: 172.20.128.179 (primary, current)
                   172.20.128.178

Reconfirmation status
-----
VMPS Action:          No Dynamic Port
```

### Configuring Dynamic Access Ports on a VMPS Client

To configure a dynamic access port on a VMPS client switch, perform this task:

|        | Command  | Purpose  |
|--------|--|--|
| Step 1 | Switch# <b>configure terminal</b>                                | Enters global configuration mode.  |
| Step 2 | Switch(config)# <b>interface</b> <i>interface</i>                | Enters interface configuration mode and specifies the port to be configured. |
| Step 3 | Switch(config-if)# <b>switchport mode access</b>                 | Sets the port to access mode.  |
| Step 4 | Switch(config-if)# <b>switchport access vlan dynamic</b>         | Configures the port as eligible for dynamic VLAN access.                     |
| Step 5 | Switch(config-if)# <b>end</b>                                    | Returns to privileged EXEC mode.   |
| Step 6 | Switch# <b>show interface</b> <i>interface</i> <b>switchport</b> | Verifies the entry.  |

This example shows how to configure a dynamic access port and to verify the entry:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fa1/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan dynamic
Switch(config-if)# end

Switch# show interface fa1/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative mode: dynamic auto
Operational Mode: dynamic access
Administrative Trunking Encapsulation: isl
Operational Trunking Encapsulation: isl
Negotiation of Trunking: Disabled
Access Mode VLAN: 0 ((Inactive))
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: NONE
Pruning VLANs Enabled: NONE
```

## Voice Ports

If a VVID (voice VLAN ID) is configured on a dynamic access port, the port can belong to both an access VLAN and a voice VLAN. Consequently, an access port configured for connecting an IP phone can have separate VLANs for the following:

- Data traffic to and from the PC that is connected to the switch through the access port of the IP phone (access VLAN)
- Voice traffic to and from the IP phone (voice VLAN)

## Reconfirming VLAN Memberships

To confirm the dynamic port VLAN membership assignments that the switch has received from the VMPS, perform this task:

|        | Command                        | Purpose  |
|--------|--------------------------------|--|
| Step 1 | Switch# <b>vmmps reconfirm</b> | Reconfirms dynamic port VLAN membership.         |
| Step 2 | Switch# <b>show vmmps</b>      | Verifies the dynamic VLAN reconfirmation status. |

## Configuring Reconfirmation Interval

VMPS clients periodically reconfirm the VLAN membership information received from the VMPS. You can set the number of minutes the VMPS client waits before reconfirming the VLAN-to-MAC-address assignments.

To configure the reconfirmation interval, perform this task:

|        | Command   | Purpose   |
|--------|---|---|
| Step 1 | Switch# <b>configure terminal</b>                     | Enters global configuration mode.   |
| Step 2 | Switch(config)# <b>vmmps reconfirm</b> <i>minutes</i> | Specifies the number of minutes between reconfirmations of the dynamic VLAN membership. |
| Step 3 | Switch(config)# <b>end</b>                            | Returns to privileged EXEC mode.  |
| Step 4 | Switch# <b>show vmmps</b>                             | Verifies the dynamic VLAN reconfirmation status.  |

This example shows how to change the reconfirmation interval to 60 minutes and verify the change:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# vmmps reconfirm 60
Switch(config)# end
Switch# show vmmps
VQP Client Status:
-----
VMPS VQP Version: 1
Reconfirm Interval: 60 min
Server Retry Count: 10
VMPS domain server: 172.20.130.50 (primary, current)

Reconfirmation status
-----
VMPS Action:          No Host
```

## Configuring the Retry Interval

You can set the number of times that the VMPS client attempts to contact the VMPS before querying the next server.

To configure the retry interval, perform this task:

|        | Command                                  | Purpose   |
|--------|--|---|
| Step 1 | Switch# <b>configure terminal</b>        | Enters global configuration mode.   |
| Step 2 | Switch(config)# <b>vmmps retry count</b> | Specifies the retry count for the VPQ queries. Default is 3. Range is from 1 to 10. |
| Step 3 | Switch(config)# <b>end</b>               | Returns to privileged EXEC mode.  |
| Step 4 | Switch# <b>show vmmps</b>                | Verifies the retry count.   |

This example shows how to change the retry count to 5 and to verify the change:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# vmmps retry 5
Switch(config)# end

Switch# show vmmps
VQP Client Status:
-----
VMPS VQP Version: 1
Reconfirm Interval: 60 min
Server Retry Count: 5
VMPS domain server: 172.20.130.50 (primary, current)

Reconfirmation status
-----
VMPS Action:          No Host
```

## Administering and Monitoring the VMPS

You can display the following information about the VMPS with the **show vmmps** command:

|                    |   |
|--------------------|---|
| VQP Version        | The version of VQP used to communicate with the VMPS. The switch queries the VMPS 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 currently sends queries to the one marked “current.” The one marked “primary” is the primary server.   |
| VMPS Action        | The result of the most-recent reconfirmation attempt. This action can occur automatically when the reconfirmation interval expired, or you can force it by entering the <b>vmmps reconfirm</b> command or its CVSM or SNMP equivalent. |

The following example shows how to display VMPS information:

```
Switch# show vmmps
VQP Client Status:
-----
VMPS VQP Version: 1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server:
```

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

The following example shows how to display VMPS statistics:

```
Switch# show vmmps statistics
VMPS Client Statistics
-----
VQP Queries:          0
VQP Responses:       0
VMPS Changes:        0
VQP Shutdowns:      0
VQP Denied:          0
VQP Wrong Domain:   0
VQP Wrong Version:  0
VQP Insufficient Resource: 0
```



**Note**

---

Refer to the *Cisco IOS Command Reference* for details on VMPS statistics.

---

## Troubleshooting Dynamic Port VLAN Membership

VMPS errdisables a dynamic port under the following conditions:

- The VMPS is in secure mode, and it does not allow the host to connect to the port. The VMPS errdisables the port to prevent the host from connecting to the network.
- More than 50 active hosts reside on a dynamic port.

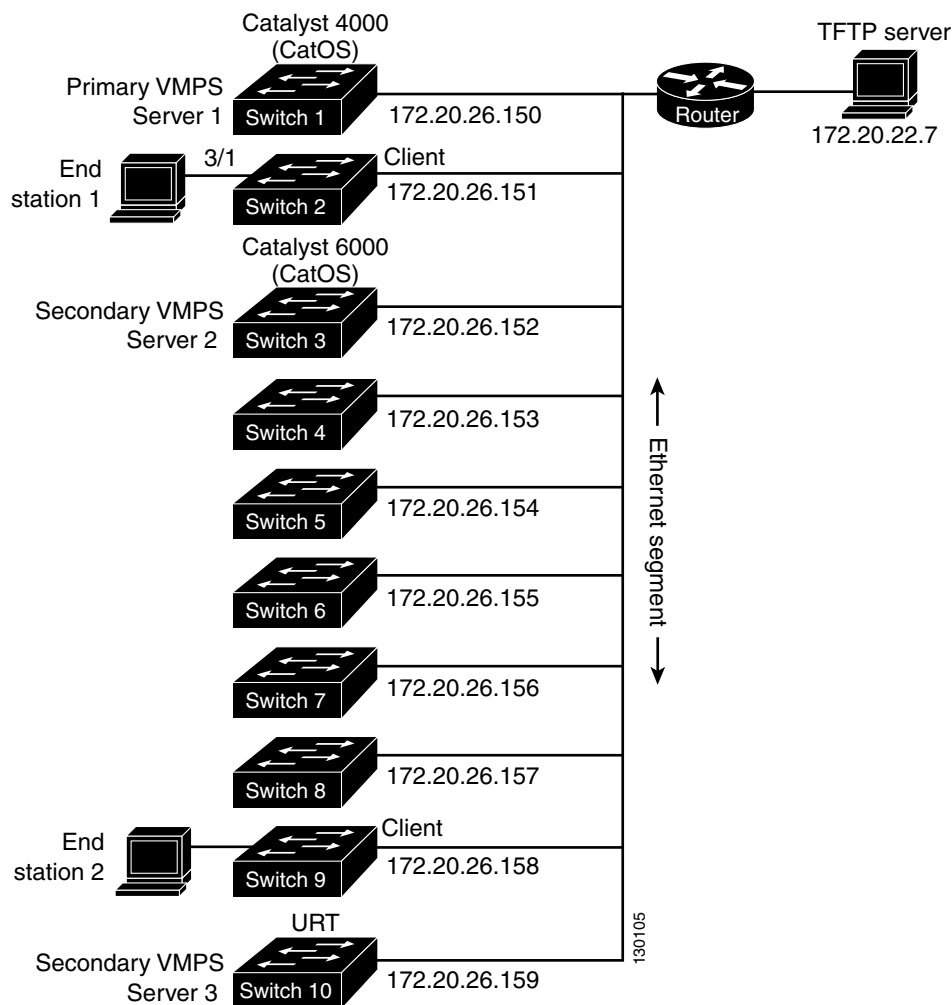
For information on how to display the status of interfaces in error-disabled state, refer to [Chapter 9, “Checking Port Status and Connectivity.”](#) To recover an errdisabled port, use the **errdisable recovery cause vmpps** global configuration command.

## Dynamic Port VLAN Membership Configuration Example

Figure 16-4 on page 16-29 shows a network with a VMPS servers and VMPS client switches with dynamic ports. In this example, these assumptions apply:

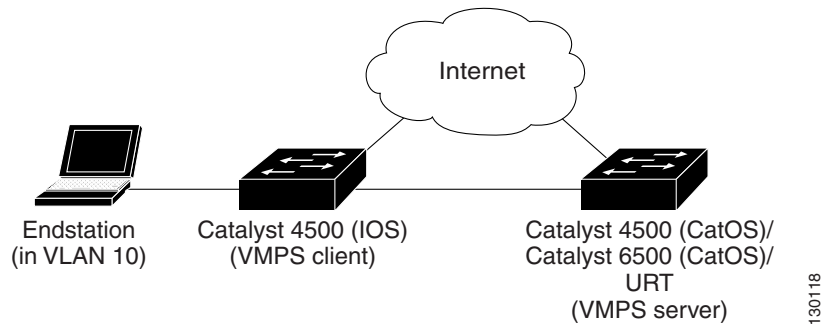
- The VMPS server and the VMPS client are separate switches.
- The Catalyst 4000 family Switch 1 (running Catalyst Operating System) is the primary VMPS server.
- The Catalyst 6000 family Switch 3 (running Catalyst Operating System) and the URT are secondary VMPS servers.
- End stations are connected to these clients:
  - Catalyst 4500 series XL Switch 2 (running Catalyst Cisco IOS)
  - Catalyst 4500 series XL Switch 9 (running Catalyst Cisco IOS)
- The database configuration file is called Bldg-G.db and is stored on the TFTP server with the IP address 172.20.22.7.

**Figure 16-4** Dynamic Port VLAN Membership Configuration

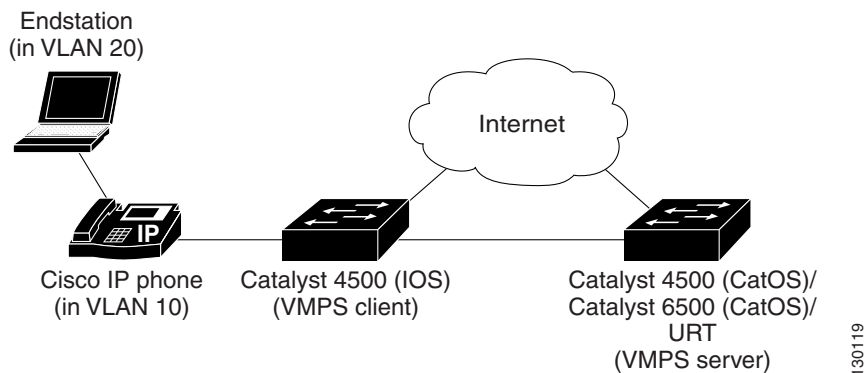


Two topologies are possible. Figure 16-5 illustrates a topology with one end station attached directly to a Catalyst 4500 series switch operating as a VMPS client. Figure 16-6 illustrates a topology with an end station attached to a Cisco IP Phone, which is attached to a Catalyst 4500 series switch.

**Figure 16-5** Topology with an End Station Attached Directly to a Catalyst 4500 Series Switch Operating as a VMPS Client



**Figure 16-6** Topology with an End Station Attached to a Cisco IP Phone that is Attached to a Catalyst 4500 Series Switch



In the following procedure, the Catalyst 4500 and Catalyst 6500 series switches (running Catalyst Operating System) are the VMPS servers. Use this procedure to configure the Catalyst 4500 series switch clients in the network:

- 
- Step 1** Configure the VMPS server addresses on Switch 2, the client switch.
- a. Starting from privileged EXEC mode, enter global configuration mode:
 

```
switch# configuration terminal
```
  - b. Enter the primary VMPS server IP address:
 

```
switch(config)# vmps server 172.20.26.150 primary
```
  - c. Enter the secondary VMPS server IP addresses:
 

```
switch(config)# vmps server 172.20.26.152
```
  - d. To verify your entry of the VMPS IP addresses, return to privileged EXEC mode:
 

```
switch(config)# exit
```

- e. Display VMPS information configured for the switch:

```
switch# show vmps
VQP Client Status:
-----
VMPS VQP Version: 1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server: 172.20.26.152
                    172.20.26.150 (primary, current)
```

- Step 2** Configure port Fa0/1 on Switch 2 as a dynamic port.

- a. Return to global configuration mode:

```
switch# configure terminal
```

- b. Enter interface configuration mode:

```
switch(config)# interface fa2/1
```

- c. Configure the VLAN membership mode for static-access ports:

```
switch(config-if)# switchport mode access
```

- d. Assign the port dynamic VLAN membership:

```
switch(config-if)# switchport access vlan dynamic
```

- e. Return to privileged EXEC mode:

```
switch(config-if)# exit
switch#
```

- Step 3** Connect End Station 2 on port Fa2/1. When End Station 2 sends a packet, Switch 2 sends a query to the primary VMPS server, Switch 1. Switch 1 responds with the VLAN ID for port Fa2/1. If spanning-tree PortFast mode is enabled on Fa2/1, port Fa2/1 connects immediately and begins forwarding.

- Step 4** Set the VMPS reconfirmation period to 60 minutes. The reconfirmation period is the number of minutes the switch waits before reconfirming the VLAN to MAC address assignments.

```
switch# config terminal
switch(config)# vmps reconfirm 60
```

- Step 5** Confirm the entry from privileged EXEC mode:

```
switch# show vmps
VQP Client Status:
-----
VMPS VQP Version: 1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server:

Reconfirmation status
-----
VMPS Action:          No Dynamic Port
```

- Step 6** Repeat Steps 1 and 2 to configure the VMPS server addresses, and assign dynamic ports on each VMPS client switch.

## VMPS Database Configuration File Example

This example shows a sample VMPS database configuration file as it appears on a VMPS server. A VMPS database configuration file is an ASCII text file that is stored on a TFTP server accessible to the switch that functions as the VMPS server.

```
!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 WBU
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.cccd.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 Fa1/3
  device 172.20.26.141 port Fa1/4
vmps-port-group "Executive Row"
  device 198.4.254.222 port es5%Fa0/1
  device 198.4.254.222 port es5%Fa0/2
  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
!
```



```
!vmports-policies {vlan-name <vlan_name> | vlan-group <group-name>}
! {port-group <group-name> | device <device-id> port <port-name>}
!
vmports-policies vlan-group Engineering
  port-group WiringCloset1
vmports-policies vlan-name Green
  device 198.92.30.32 port Fa0/9
vmports-policies vlan-name Purple
  device 198.4.254.22 port Fa0/10
  port-group "Executive Row"
```

