



CHAPTER 13

Configuring VTP

This chapter describes how to configure the VLAN Trunking Protocol (VTP) on the Cisco 7600 series routers.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the Cisco 7600 Series Routers Command References at this URL:

http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html

This chapter consists of these sections:

- [Understanding How VTP Works, page 13-1](#)
- [VTP Default Configuration, page 13-6](#)
- [VTP Configuration Guidelines and Restrictions, page 13-6](#)
- [Configuring VTP, page 13-8](#)

Understanding How VTP Works

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 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.



Note

For complete information on configuring VLANs, see [Chapter 14, “Configuring VLANs.”](#)

These sections describe how VTP works:

- [Understanding the VTP Domain, page 13-2](#)
- [Understanding VTP Modes, page 13-2](#)
- [Understanding VTP Advertisements, page 13-3](#)

- [Understanding VTP Versions, page 13-3](#)
- [Understanding VTP Pruning, page 13-5](#)

Understanding the VTP Domain

A VTP domain (also called a VLAN management 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 one and 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 Cisco 7600 series router is in VTP server mode and is in the no-management domain state until the router receives an advertisement for a domain over a trunk link or you configure a management domain.

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

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

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 trunk connections.

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

Understanding VTP Modes

You can configure a Cisco 7600 series router 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**—In VTP version 1, 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 and VTP version 3, transparent network devices do forward VTP advertisements that they receive out their trunking LAN ports.
- **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**

Cisco 7600 series routers automatically change from VTP server mode to VTP client mode if the router detects a failure while writing configuration to nonvolatile random-access memory (NVRAM). If this happens, the router 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 port 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 (Inter-Switch Link [ISL] and IEEE 802.1Q)
- Emulated LAN names (for ATM LAN Emulation Services [LANE])
- IEEE 802.10 Security Association Identifier (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

If you use VTP in your network, you must decide whether to use VTP version 1, version 2, or version 3.

**Note**

If you are using VTP in a Token Ring environment, you must use version 2 or version 3.

VTP 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, see the [“Understanding How VLANs Work” section on page 14-1](#).
- 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, a VTP transparent network device 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 supervisor engine software, VTP version 2 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**—VTP version 3 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.

- **Support for extended VLAN Database Propagation**—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 Cisco 7600 series routers 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 via 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 13-13](#).)

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, it is possible to 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, unknown, and flooded 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 support VTP pruning. On devices that do not support VTP pruning, you must manually configure the VLANs allowed on trunks.

Figure 13-1 shows a switched network without VTP pruning enabled. Interface 1 on network Switch 1 and port 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 ports in the Red VLAN.

You enable pruning globally on the Cisco 7600 series router (see the “[Enabling VTP Pruning](#)” section on page 13-9). You configure pruning on Layer 2 trunking LAN ports (see the “[Configuring LAN Interfaces for Layer 2 Switching](#)” section on page 10-6).

Figure 13-1 Flooding Traffic without VTP Pruning

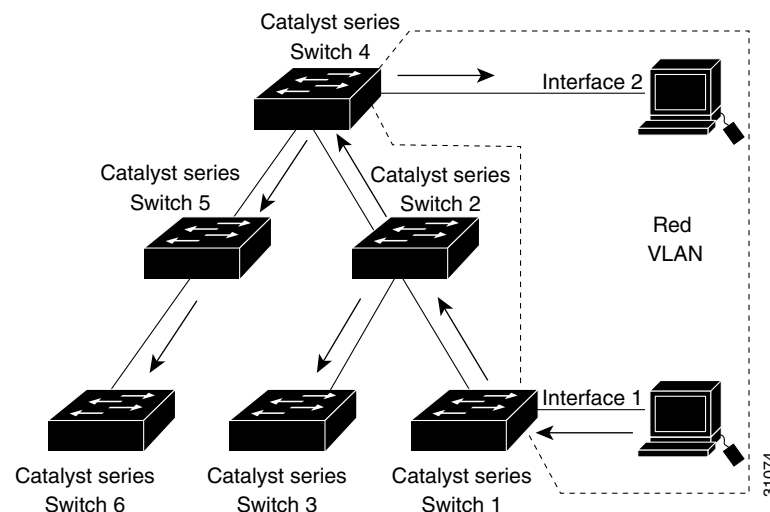
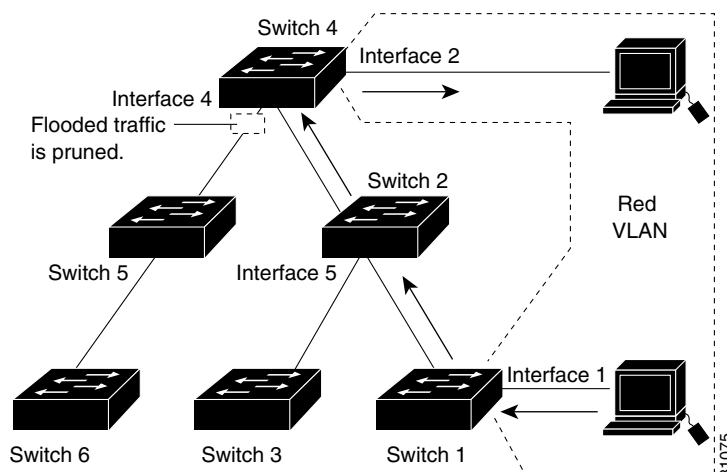


Figure 13-2 shows the same switched network with VTP pruning enabled. The broadcast traffic from Switch 1 is not forwarded to Switches 3, 5, and 6 because traffic for the Red VLAN has been pruned on the links indicated (port 5 on Switch 2 and port 4 on Switch 4).

Figure 13-2 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 pruning eligible. VTP pruning does not prune traffic from pruning-ineligible VLANs. VLAN 1 is always pruning ineligible; traffic from VLAN 1 cannot be pruned.

To configure VTP pruning on a trunking LAN port, use the **switchport trunk pruning vlan** command (see the “[Configuring LAN Interfaces for Layer 2 Switching](#)” section on page 10-6). VTP pruning operates when a LAN port is trunking. You can set VLAN pruning eligibility whether VTP pruning is enabled or disabled for the VTP domain, whether any given VLAN exists or not, and whether the LAN port is currently trunking or not.

VTP Default Configuration

Table 13-1 shows the default VTP configuration.

Table 13-1 VTP Default Configuration

Feature	Default Value
VTP domain name	Null
VTP mode	Server
VTP version	Version 1
VTP password	None
VTP pruning	Disabled

VTP Configuration Guidelines and Restrictions

When implementing VTP in your network, follow these guidelines and restrictions:

- Supervisor engine redundancy does not support nondefault VLAN data file names or locations. Do not enter the **vtp file file_name** command on a router that has a redundant supervisor engine.
- Before installing a redundant supervisor engine, enter the **no vtp file** command to return to the default configuration.

- 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 in secure mode.

**Caution**

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

- A VTP version-2-capable network device can operate in the same VTP domain as a network device running VTP version 1 provided 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 network device, all of the version-2-capable network devices in the domain enable VTP version 2.
- When a VTP version 3 device on a trunk port receives messages from a VTP version 2 device, it will send a scaled-down version of the VLAN database on that particular trunk in a VTP version 2 format. A VTP version 3 device will 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 will continue 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 will not accept configuration information from a VTP version 2 or version 1 device.
- Unlike in VTP version 2, when VTP is configured to be version 3, this will not configure all the version-3-capable devices in the domain to start behaving as VTP 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.
- When you enable or disable VTP pruning on a VTP server, VTP pruning for the entire management domain is enabled or disabled.
- The pruning-eligibility configuration applies globally to all trunks on the router. You cannot configure pruning-eligibility separately for each trunk.
- When you configure VLANs as pruning eligible or pruning ineligible, pruning eligibility for those VLANs is affected on that router only, not on all network devices in the VTP domain.
- In VTP version 1 and version 2, VTP does not propagate configuration information for extended-range VLANs (VLAN numbers 1006 to 4094). You must configure extended-range VLANs manually on each network device.
- If there is insufficient DRAM available for use by VTP, the VTP mode changes to transparent.
- Network devices in VTP transparent mode do not send VTP Join messages. On Cisco 7600 series routers with trunk connections to network devices in VTP transparent mode, configure the VLANs that are used by the transparent-mode network devices or that need to be carried across trunks as pruning ineligible. For information about configuring prune eligibility, see the [“Configuring the List of Prune-Eligible VLANs” section on page 10-11](#).

- 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.

Configuring VTP

These sections describe how to configure VTP:

- [Configuring VTP Global Parameters, page 13-8](#)
- [Configuring the VTP Mode, page 13-10](#)
- [Starting a Takeover, page 13-13](#)
- [Displaying VTP Statistics, page 13-13](#)
- [Displaying VTP Devices in a Domain, page 13-14](#)

Configuring VTP Global Parameters

These sections describe configuring the VTP global parameters:

- [Configuring a VTP Password, page 13-8](#)
- [Enabling VTP Pruning, page 13-9](#)
- [Enabling the VTP Version Number, page 13-10](#)



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
Router(config)# vtp password <i>password_string</i> [hidden secret]	Sets a password, which can be from 8 to 64 characters long, for the VTP domain. In VTP version 3 the keywords hidden and secret are available. • If the hidden keyword is used, the secret key generated from the password string is saved in the const_nvram:vlan.dat file. If a takeover command is issued, that password must be reentered. • If the secret keyword is used, the password secret key can be directly configured. The secret password must contain 32 hexadecimal characters.
Router(config)# no vtp password	Clears the password.

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

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

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

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



Note

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

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

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

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

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

Enabling VTP Pruning

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

	Command	Purpose
Step 1	Router(config)# vtp pruning	Enables VTP pruning in the management domain.
Step 2	Router# show vtp status include pruning	(Optional) Verifies the configuration.

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

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

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

```
Router# vtp pruning
Pruning switched ON
```

This example shows how to verify the configuration:

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

For information about configuring prune eligibility, see the [“Configuring the List of Prune-Eligible VLANs” section on page 10-11](#).

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.



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.



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 in global configuration mode:

	Command	Purpose
Step 1	Router(config)# vtp version {1 2 3}	Enables the VTP version.
Step 2	Router# show vtp status include {v1 v2 v3}	(Optional) Verifies the configuration.

This example shows one way to enable VTP version 2:

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

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

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

This example shows how to verify the configuration:

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

Configuring the VTP Mode

To configure the VTP mode, perform this task in global configuration mode:

	Command	Purpose
Step 1	Router(config)# vtp mode {client server transparent off}	Configures the VTP mode.

	Command	Purpose
Step 2	Router(config)# vtp domain <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 router has a trunk connection to a VTP domain, the router learns the domain name from the VTP server in the domain. Note You cannot clear the domain name.
Step 3	Router(config)# end	Exits VLAN configuration mode.
Step 4	Router# show vtp status	(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 router as a VTP server:

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

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

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

This example shows how to disable VTP on the router:

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

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

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

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

```
Router# 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
```

```
Router#
```

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

```
Router# 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 0x15 0x70 0x61 0xB8
                                0x24 0xB6 0x93 0x21 0x09
```

```
Router#
```

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

```
Router# 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          :
Router#
```

Starting a Takeover

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

Command	Purpose
Router# vtp primary-server [vlan mst] [force]	Changes the operational state of a router 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 hidden keyword, the user is prompted to re-enter it.) Note Using the force keyword overwrites the configuration of any conflicting servers. If not using the force keyword, you will be prompted for confirmation prior to proceeding with the takeover. Specify where to direct the takeover by selecting the appropriate feature (vlan or mst). If no feature is selected, the takeover is directed to the VLAN database.

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

```
Router# 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)
Router#
```

Displaying VTP Statistics

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

Command	Purpose
Router# show vtp counters	Displays VTP statistics.

This example shows how to display VTP statistics:

```
Router# 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
-----          -----          -----          -----
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 in privileged EXEC mode:

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

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

```

Router# 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

Router#

```