



CHAPTER 10

Configuring VTP

This chapter describes how to configure the VLAN Trunking Protocol (VTP) on the Catalyst 6500 series switches.

**Note**

For complete syntax and usage information for the commands that are used in this chapter, refer to the *Catalyst 6500 Series Switch Command Reference* publication.

This chapter consists of these sections:

- [Understanding How VTP Version 1 and Version 2 Work, page 10-1](#)
- [Default VTP Version 1 and Version 2 Configuration, page 10-5](#)
- [VTP Version 1 and Version 2 Configuration Guidelines, page 10-5](#)
- [Configuring VTP Version 1 and Version 2, page 10-6](#)
- [Understanding How VTP Version 3 Works, page 10-12](#)
- [Default VTP Version 3 Configuration, page 10-21](#)
- [Configuring VTP Version 3, page 10-22](#)

Understanding How VTP Version 1 and Version 2 Work

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

You can use VTP to manage VLANs 1–1005 in your network. (VTP version 1 and VTP version 2 do not support VLANs 1025–4094.) With VTP, you can make configuration changes centrally on one switch and have those changes automatically communicated to all the other switches in the network.

**Note**

For complete information on configuring VLANs, see [Chapter 11, “Configuring VLANs.”](#)

These sections describe how VTP works:

- [Understanding the VTP Domain, page 10-2](#)
- [Understanding VTP Modes, page 10-2](#)
- [Understanding VTP Advertisements, page 10-3](#)
- [Understanding VTP Version 2, page 10-3](#)
- [Understanding VTP Pruning, page 10-4](#)

Understanding the VTP Domain

A VTP domain (also called a VLAN management domain) is made up of one or more interconnected switches that share the same VTP domain name. A switch 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 switch is in VTP server mode and is in the no-management domain state 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 switches in the VTP domain. VTP advertisements are transmitted out all trunk connections, including Inter-Switch Link (ISL), IEEE 802.1Q, IEEE 802.10, and ATM LAN Emulation (LANE).

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

Understanding VTP Modes

You can configure a 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 switches in the same VTP domain and synchronize their VLAN configuration with other switches based on advertisements received over trunk links. VTP server is the default mode.
- **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 switches do not participate in VTP. A VTP transparent switch does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. However, in VTP version 2, transparent switches do forward VTP advertisements that they receive out their trunk ports.
- **Off**—In the three modes described above, VTP advertisements are received and transmitted as soon as the switch enters the management domain state. In the VTP off mode, the switch behaves the same as in VTP transparent mode with the exception that VTP advertisements are not forwarded.

Understanding VTP Advertisements

Each switch in the VTP domain sends periodic advertisements out each trunk port to a reserved multicast address. VTP advertisements are received by neighboring switches, 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 the maximum transmission unit (MTU) size for each VLAN
- Frame format

Understanding VTP Version 2

If you use VTP in your network, you must decide whether to use VTP version 1, version 2, or version 3 (for details on version 3, see the [“Understanding How VTP Version 3 Works”](#) section on page 10-12).



Note

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

VTP version 2 supports the following features that are 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 [Chapter 11, “Configuring VLANs.”](#)
- **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 switch inspects VTP messages for the domain name and version and forwards a message only if the version and domain name match. Since 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.

Understanding VTP Pruning



Note

Enabling VTP pruning on a VTP version 3 switch enables pruning only on the switch that you enable it on. VTP pruning is not propagated as it is with VTP version 1 and VTP version 2.

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.

Make sure that all devices in the management domain support VTP pruning before enabling it. VTP pruning is supported in supervisor engine software release 5.1(1) and later releases.



Note

If you use routers to route between emulated LANs, you should disable VTP pruning in the VTP management domain that contains the switches with ATM LANE modules installed (VTP pruning messages are sent over the ATM LANE module because it is a trunk). You can also disable pruning for the LANE VLANs by using the `clear vtp pruneeligible` command on all switches with ATM LANE modules.

Figure 10-1 shows a switched network without VTP pruning enabled. Port 1 on Switch 1 and port 2 on Switch 4 are assigned to the Red VLAN. A broadcast is sent from the host that is connected to Switch 1. Switch 1 floods the broadcast and every switch in the network receives it even though Switches 3, 5, and 6 have no ports in the Red VLAN.

Figure 10-1 Flooding Traffic without VTP Pruning

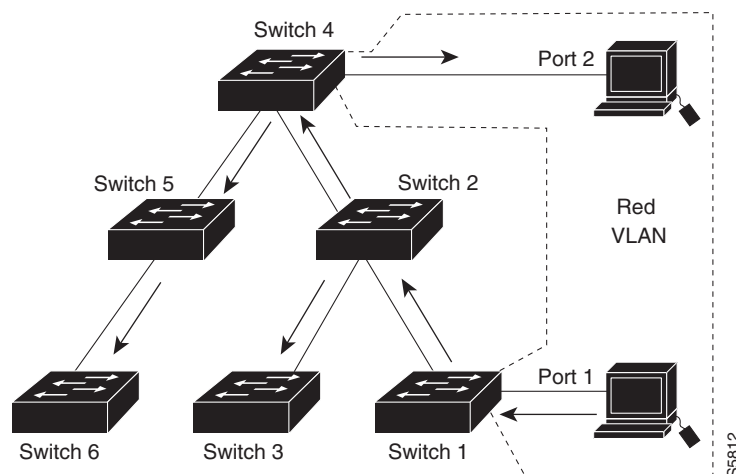
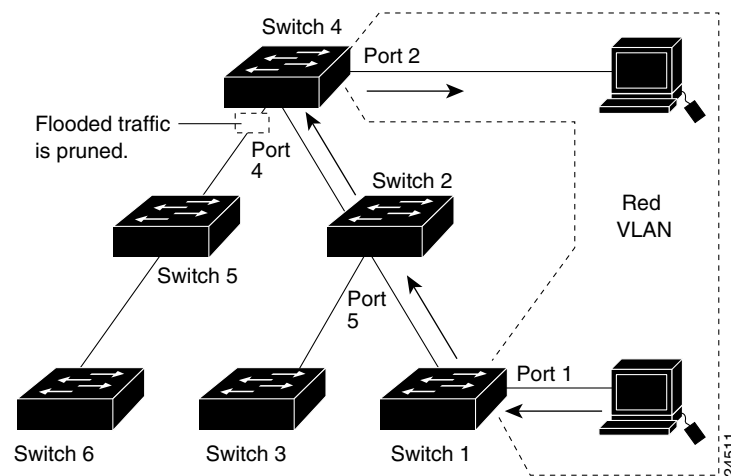


Figure 10-2 shows the same switched network with VTP pruning enabled. The broadcast traffic from Switch 1 is not forwarded to Switches 3, 5, and 6 because traffic for the Red VLAN has been pruned on the links indicated (port 5 on Switch 2 and port 4 on Switch 4).

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 2–1000 are pruning eligible. VTP pruning does not prune traffic from VLANs that are pruning ineligible. VLAN 1 is always pruning ineligible; traffic from VLAN 1 cannot be pruned.

To make a VLAN pruning ineligible, enter the **clear vtp pruneeligible** command. To make a VLAN pruning eligible again, enter the **set vtp pruneeligible** command. You can set VLAN pruning eligibility regardless of whether VTP pruning is enabled or disabled for the domain. Pruning eligibility always applies to the local device only, not for the entire VTP domain.

Figure 10-2 Flooding Traffic with VTP Pruning



Default VTP Version 1 and Version 2 Configuration

Table 10-1 shows the default VTP configuration.

Table 10-1 VTP Default Configuration

Feature	Default Value
VTP domain name	Null
VTP mode	Server
VTP version 2 enable state	Version 1 is enabled (version 2 is disabled)
VTP password	None
VTP pruning	Disabled

VTP Version 1 and Version 2 Configuration Guidelines

This section describes the guidelines for implementing VTP in your network:

- All switches in a VTP domain must run the same VTP version.
- You must configure a password on each switch in the management domain when you are 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 switch in the domain.

- A VTP version 2-capable switch can operate in the same VTP domain as a switch running VTP version 1 if VTP version 2 is disabled on the VTP version 2-capable switch (VTP version 2 is disabled by default).
- Do not enable VTP version 2 on a switch unless all of the switches in the same VTP domain are version 2 capable. When you enable VTP version 2 on a switch, all of the version 2-capable switches in the domain enable VTP version 2.
- In a Token Ring environment, you must enable VTP version 2 for Token Ring VLAN switching to function properly.
- Enabling or disabling VTP pruning on a VTP server enables or disables VTP pruning for the entire management domain.
- Making VLANs pruning eligible or pruning ineligible on a switch affects pruning eligibility for those VLANs on that device only (not on all switches in the VTP domain).
- With software release 8.1(1), all VTP versions can be configured on a per-port basis. See the [“VTP Version 3 Per-Port Configuration”](#) section on page 10-14.

Configuring VTP Version 1 and Version 2

These sections describe how to configure VTP:

- [Configuring a VTP Server, page 10-6](#)
- [Configuring a VTP Client, page 10-7](#)
- [Configuring VTP \(VTP Transparent Mode\), page 10-8](#)
- [Disabling VTP Using the Off Mode, page 10-8](#)
- [Enabling VTP Version 2, page 10-9](#)
- [Disabling VTP Version 2, page 10-10](#)
- [Enabling VTP Pruning, page 10-10](#)
- [Disabling VTP Pruning, page 10-12](#)
- [Displaying VTP Statistics, page 10-12](#)

Configuring a VTP Server

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

To configure the switch as a VTP server, perform this task in privileged mode:

	Task	Command
Step 1	Define the VTP domain name.	set vtp domain <i>name</i>
Step 2	Place the switch in VTP server mode.	set vtp mode server
Step 3	(Optional) Set a password for the VTP domain.	set vtp passwd <i>passwd</i>
Step 4	Verify the VTP configuration.	show vtp domain

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

```

Console> (enable) set vtp domain Lab_Network
VTP domain Lab_Network modified
Console> (enable) set vtp mode server
Changing VTP mode for all features
VTP domain Lab_Network modified
Console> (enable) show vtp domain
Version      : running VTP2 (VTP3 capable)
Domain Name  : Lab_Network                Password  : configured (hidden)
Notifications: disabled                  Updater ID: 172.20.52.19

Feature      Mode      Revision
-----
VLAN         Server    0

Pruning      : disabled
VLANs prune eligible: 2-1000
Console> (enable)

```

Configuring a VTP Client

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

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

	Task	Command
Step 1	Define the VTP domain name.	set vtp domain <i>name</i>
Step 2	Place the switch in VTP client mode.	set vtp mode client
Step 3	Verify the VTP configuration.	show vtp domain

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

```

Console> (enable) set vtp domain Lab_Network
VTP domain Lab_Network modified
Console> (enable) set vtp mode client
Changing VTP mode for all features
VTP domain Lab_Network modified
Console> (enable) show vtp domain
Version      : running VTP2 (VTP3 capable)
Domain Name  : Lab_Network                Password  : configured (hidden)
Notifications: disabled                  Updater ID: 172.20.52.19

Feature      Mode      Revision
-----

```

```

VLAN          Client          0

Pruning              : disabled
VLANs prune eligible: 2-1000
Console> (enable)

```

Configuring VTP (VTP Transparent Mode)

When you configure the switch as VTP transparent, you disable VTP on the switch. A VTP transparent switch does not send VTP updates and does not act on VTP updates that are received from other switches. However, a VTP transparent switch running VTP version 2 does forward received VTP advertisements out all of its trunk links.



Note

Network devices in VTP transparent mode do not send VTP join messages. On Catalyst 6500 series switches 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 (use the **clear vtp pruneeligible** command).

To disable VTP on the switch, perform this task in privileged mode:

	Task	Command
Step 1	Disable VTP on the switch by configuring it for VTP transparent mode.	set vtp mode transparent
Step 2	Verify the VTP configuration.	show vtp domain

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

```

Console> (enable) set vtp mode transparent
Changing VTP mode for all features
VTP domain Lab_Net modified
Console> (enable) show vtp domain
Version          : running VTP2 (VTP3 capable)
Domain Name     : Lab_Network
Notifications: disabled
Password        : configured (hidden)
Updater ID     : 172.20.52.19

Feature          Mode          Revision
-----
VLAN             Transparent  0

Pruning              : disabled
VLANs prune eligible: 2-1000
Console> (enable)

```

Disabling VTP Using the Off Mode

When you disable VTP using the off mode, the switch behaves the same as in VTP transparent mode with the exception that VTP advertisements are not forwarded.

To disable VTP using the off mode, perform this task in privileged mode:

	Task	Command
Step 1	Disable VTP using the off mode.	set vtp mode off
Step 2	Verify the VTP configuration.	show vtp domain

This example shows how to disable VTP using the off mode:

```

Console> (enable) set vtp mode off
Changing VTP mode for all features
VTP domain Lab_Net modified
Console> (enable) show vtp domain
Version      : running VTP2 (VTP3 capable)
Domain Name  : Lab_Network                Password  : configured (hidden)
Notifications: disabled                  Updater ID: 172.20.52.19

Feature      Mode      Revision
-----
VLAN         Off      0

Pruning      : disabled
VLANs prune eligible: 2-1000
Console> (enable)

```

Enabling VTP Version 2

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



Caution

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



Note

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

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

	Task	Command
Step 1	Enable VTP version 2 on the switch.	set vtp version 2
Step 2	Verify that VTP version 2 is enabled.	show vtp domain

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

```

Console> (enable) set vtp version 2
This command will enable VTP version 2 function in the entire management domain.
All devices in the management domain should be version2-capable before enabling.
Do you want to continue (y/n) [n]? y
VTP domain server modified
Console> (enable) show vtp domain

```

```

Version      : running VTP2 (VTP3 capable)
Domain Name  : Lab_Network
Notifications: disabled
Password    : configured (hidden)
Updater ID: 172.20.52.19

Feature      Mode      Revision
-----
VLAN         Off       0

Pruning      : disabled
VLANs prune eligible: 2-1000
Console> (enable)

```

Disabling VTP Version 2

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

	Task	Command
Step 1	Disable VTP version 2.	set vtp version 1
Step 2	Verify that VTP version 2 is disabled.	show vtp domain

This example shows how to disable VTP version 2:

```

Console> (enable) set vtp version 1
This command will enable VTP version 1 function in the entire management domain.
Warning: trbrf & trcrf vlans will not work properly in this version.
Do you want to continue (y/n) [n]? y
VTP domain Lab_Network modified
Console> (enable) show vtp domain
Version      : running VTP1 (VTP3 capable)
Domain Name  : Lab_Network
Notifications: disabled
Password    : configured (hidden)
Updater ID: 172.20.52.19

Feature      Mode      Revision
-----
VLAN         Off       0

Pruning      : disabled
VLANs prune eligible: 2-1000
Console> (enable)

```

Enabling VTP Pruning

To enable VTP pruning, perform this task in privileged mode:

	Task	Command
Step 1	Enable VTP pruning in the management domain.	set vtp pruning enable
Step 2	(Optional) Make specific VLANs pruning ineligible on the device. (By default, VLANs 2–1000 are pruning eligible.)	clear vtp pruneeligible <i>vlan_range</i>
Step 3	(Optional) Make specific VLANs pruning eligible on the device.	set vtp pruneeligible <i>vlan_range</i>

	Task	Command
Step 4	Verify the VTP pruning configuration.	show vtp domain
Step 5	Verify that the appropriate VLANs are being pruned on trunk ports.	show trunk

This example shows how to enable VTP pruning in the management domain and how to make VLANs 2–99, 250–255, and 501–1000 pruning eligible on the particular device:

```

Console> (enable) set vtp pruning enable
Cannot modify pruning mode unless in VTP SERVER mode.

Console> (enable) set vtp mode server
Changing VTP mode for all features
VTP domain Lab_Network modified

Console> (enable) set vtp pruning enable
This command will enable the pruning function in the entire management domain.
All devices in the management domain should be pruning-capable before enabling.
Do you want to continue (y/n) [n]? y
VTP domain Lab_Network modified

Console> (enable) clear vtp pruneeligible 100-500
Vlans 1,100-500,1001-1023 will not be pruned on this device.
VTP domain Lab_Network modified.

Console> (enable) set vtp pruneeligible 250-255
Vlans 2-99,250-255,501-1000,1024-4094 eligible for pruning on this device.
VTP domain Lab_Network modified.

Console> (enable) show vtp domain
Version      : running VTP1 (VTP3 capable)
Domain Name  : Lab_Network
Notifications: disabled
Password    : configured (hidden)
Updater ID  : 172.20.52.19

Feature      Mode      Revision
-----
VLAN         Server    1

Pruning      : enabled
VLANs prune eligible: 2-99,250-255,501-1000

Console> (enable) show trunk
* - indicates vtp domain mismatch
# - indicates dot1q-all-tagged enabled on the port
Port      Mode      Encapsulation  Status      Native vlan
-----
16/1      nonegotiate  isl            trunking    1

Port      Vlans allowed on trunk
-----
16/1      1-1005,1025-4094

Port      Vlans allowed and active in management domain
-----
16/1

Port      Vlans in spanning tree forwarding state and not pruned
-----
16/1
Console> (enable)

```

Disabling VTP Pruning

To disable VTP pruning, perform this task in privileged mode:

	Task	Command
Step 1	Disable VTP pruning in the management domain.	set vtp pruning disable
Step 2	Verify that VTP pruning is disabled.	show vtp domain

This example shows how to disable VTP pruning in the management domain:

```

Console> (enable) set vtp pruning disable
This command will disable the pruning function in the entire management domain.
Do you want to continue (y/n) [n]? y
VTP domain Lab_Network modified
Console> (enable)

```

Displaying VTP Statistics

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

Task	Command
Display VTP statistics for the switch.	show vtp statistics

This example shows how to display VTP statistics on the switch:

```

Console> (enable) show vtp statistics
VTP statistics:
summary advts received          0
subset advts received           0
request advts received          0
summary advts transmitted       7843
subset advts transmitted        4
request advts transmitted       20
No of config revision errors    0
No of config digest errors      0

VTP pruning statistics:

Trunk   Join Transmitted Join Received Summary advts received from GVRP PDU
non-pruning-capable device Received
-----
16/1    75                0                0                0
Console> (enable)

```

Understanding How VTP Version 3 Works

VTP version 3 differs from earlier VTP versions in that it does not directly handle VLANs. VTP version 3 is a protocol that is only responsible for distributing a list of opaque databases over an administrative domain. When enabled, VTP version 3 provides these enhancements to previous VTP versions:

- Support for extended VLANs.
- Support for the creation and advertising of private VLANs.
- Support for VLAN instances and MST mapping propagation instances.
- Improved server authentication.
- Protection from the “wrong” database accidentally being inserted into a VTP domain.
- Interaction with VTP version 1 and VTP version 2.
- Ability to be configured on a per-port basis.



Note With software release 8.1(1), all VTP versions can be configured on a per-port basis.

- Provides the ability to propagate the VLAN database *and* other databases. VTP version 3 is a collection of protocol *instances*, with each instance handling one database that is associated with a given feature. VTP version 3 handles the configuration propagation of multiple databases (features) independent of one another by running multiple instances of the protocol.



Note In software releases 8.1(x) and 8.2(x), the only supported database propagation is for the VLAN database. In software release 8.3(1), support is added to propagate the MST database.

These sections describe VTP version 3:

- [VTP Version 3 Authentication, page 10-13](#)
- [VTP Version 3 Per-Port Configuration, page 10-14](#)
- [VTP Version 3 Domains, Modes, and Partitions, page 10-14](#)
- [VTP Version 3 Modes, page 10-17](#)
- [VTP Version 3 Databases, page 10-19](#)

VTP Version 3 Authentication

VTP version 3 introduces an enhancement to the handling of VTP passwords. VTP version 3 allows the configuration of a *primary server*. A VTP version 3 server cannot make any configuration changes in the domain without first becoming the primary server for the domain. The VTP version 3 authentication enhancements are as follows:

- If no password is configured or if a password is configured the same way as in VTP version 1 or VTP version 2 (without using the **hidden** or **secret** keywords), the following occurs:
 - A switch can become the primary server and configure the domain with no restriction.
 - The password appears in the configuration.

This enhancement is equivalent to the existing VTP version 1 and VTP version 2 levels of security.

- If a password is configured as hidden using the **hidden** password configuration option, the following occurs:
 - The password does not appear in plain text in the configuration; the *secret* hexadecimal format of the password is saved in the configuration.

- If you try to configure the switch as a primary server, you are prompted for the password. If your password matches the secret password, the switch becomes a primary server allowing you to configure the domain.

For more information on configuring the passwords, see the [“Configuring VTP Version 3 Passwords” section on page 10-26](#).

VTP Version 3 Per-Port Configuration



Note

With software release 8.1(1), all VTP versions can be configured on a per-port basis.

VTP version 3 allows you to disable the protocol on a per-port basis. If a trunk is connected to a switch or server that is not trusted and is not supposed to interact with the VTP domain, it is now possible to drop incoming VTP packets and prevent VTP advertisements on a particular trunk. This configuration option has no impact on other protocols.

For more information on the per-port configuration options, see the [“Disabling VTP Version 3 on a Per-Port Basis” section on page 10-28](#).

VTP Version 3 Domains, Modes, and Partitions

This section describes how the domains, modes, and partitions are handled in VTP version 3 as compared to VTP versions 2 and 3:

- A VTP version 3 server can be configured as primary or secondary.
- The VTP version 3 modes (server, client, and transparent) are specific to a VTP instance.
- A VTP version 3 domain can be partitioned.

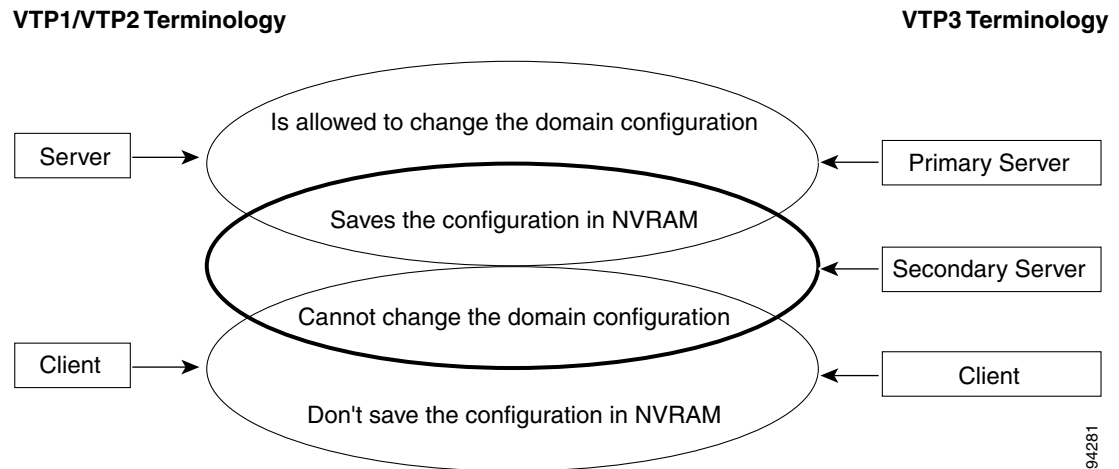
For more information about these features, see these sections:

- [Primary Servers, Secondary Servers, and Clients, page 10-14](#)
- [Partitioned VTP Domains, page 10-15](#)
- [Reconfiguring a Partitioned VTP Domain, page 10-16](#)

Primary Servers, Secondary Servers, and Clients

In previous VTP implementations, the VTP server could modify and store the VTP domain configuration in NVRAM, and a VTP client could only receive the configuration from the network and could not save or modify it.

In VTP version 3, the primary server functions the same way as the VTP version 1 and version 2 servers, and the secondary server can store the configuration of the domain but cannot modify it. The concept of client is unchanged in VTP version 3 (see [Figure 10-3](#)). The main distinction in VTP version 3 is that the server, client, and transparent modes are specific to a VTP instance. For example, in VTP version 3, it is possible for a switch to be a primary server for one instance and a client for another instance.

Figure 10-3 VTP Version 3: Primary Servers, Secondary Servers, and Clients

Partitioned VTP Domains

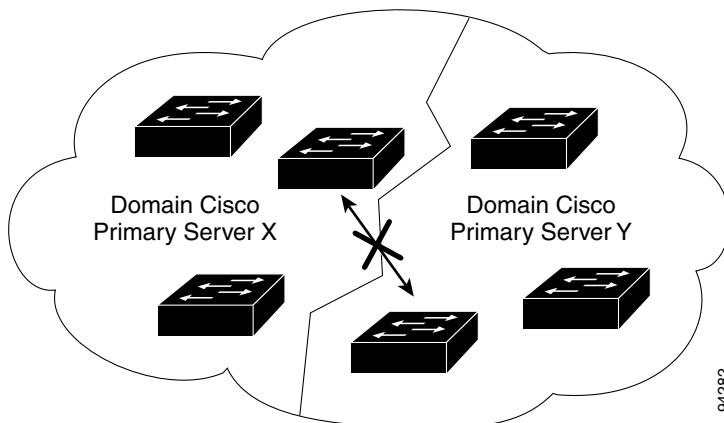
VTP version 3 restricts the configuration rights for a domain to a unique primary server, as follows:

- VTP configuration is possible only on a primary server.
- The identifier (ID) of the primary server that generated the database is attached to the VTP advertisements.
- A VTP switch keeps the ID of a primary server and accepts VTP database updates from its current primary server only.

Because the ID of a primary server is always sent with the VTP configuration, any switch that has a configuration also knows the corresponding primary server. As in VTP version 1 and VTP version 2, the switches that do not have a VTP configuration accept the first configuration that they receive (if it passes the optional authentication scheme that is described in the “[VTP Version 3 Authentication](#)” section on [page 10-13](#)). VTP version 3 switches *lock* on the primary server that generated their configuration and only listen to further VTP database updates from this primary server. This process differs significantly from VTP version 1 and VTP version 2 where a switch would always accept a superior configuration from a neighbor in the same domain. A VTP version 3 switch accepts only a superior configuration that is from the same domain *and* that is generated by the same primary server.

Ideally, there should be only one primary server in a VTP version 3 domain, but if there are several, the domain is partitioned in groups following the update of their respective primary server (see [Figure 10-4](#)). In [Figure 10-4](#), the Cisco VTP domain is partitioned between switches accepting server X or server Y as a primary server. The switches that are from different partitions do not exchange database information even though they are part of the same domain. If server X changes the VTP configuration, only the left partition of the network accepts it.

Figure 10-4 VTP Version 3: Partitioned VTP Domain



Partitions exist because of discrepancies in the domain configuration that cannot automatically be resolved by VTP. Partitions are the result of a misconfiguration or an independent configuration of a temporarily disconnected part of the domain. This behavior of VTP version 3 protects the domain from accepting a conflicting configuration after the insertion of a misconfigured switch. If a new switch is added to a domain, it will not propagate its configuration until you manually designate it as the new primary server.

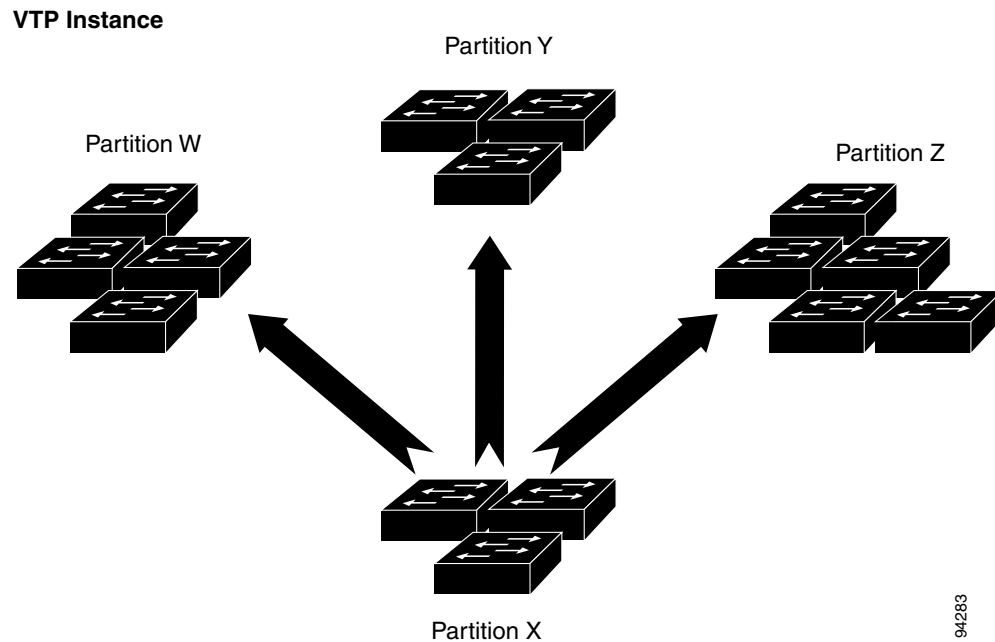
The primary server for a VLAN instance can be a different server than the primary server that is set for an MST instance. Using two primary servers in this case does not cause partitions.

For information on using the *takeover* mechanism to reconfigure partitioned VTP domains, see the [“Reconfiguring a Partitioned VTP Domain”](#) section on page 10-16.

Reconfiguring a Partitioned VTP Domain

Partitioning of a VTP domain is specific to the instance; one instance may be partitioned while another might not be partitioned. In VTP version 3, you are required to remove any partitions because the protocol cannot determine which primary server has the final, desired configuration. Figure 10-5 shows a VTP domain that has been divided into four partitions for one specific VTP instance.

In Figure 10-5, server X has the correct configuration for the domain. To reconfigure this partitioned VTP domain, you need to issue a takeover message from server X to the entire domain, advertising server X as the new primary server for this specific instance. All switches in the domain will lock onto primary server X and accept only the instance configuration updates that are initiated by server X. All switches in the domain synchronize their VTP configuration to server X for that instance.

Figure 10-5 VTP Version 3: Reconfiguring a Partitioned VTP Domain

Initiating a takeover is a critical operation due to the following reasons:

- The takeover erases conflicting configurations that are potentially stored on other primary servers in the VTP domain. VTP lists all the switches with conflicting configurations (when you enter the **show vtp conflicts** command) and prompts you for confirmation before taking over (a server has conflicting information if it belongs to the same VTP domain but has a different primary server).
- The takeover leaves this switch (server X in [Figure 10-5](#)) as the only primary server controlling the VTP domain.

If you have a hidden password configured, you need to reenter the password to do a takeover. Switches refuse the takeover request if they are not correctly authenticated. If no authentication is enabled, any server is able to take over.

After a takeover, there should be only one primary server controlling the entire VTP domain for a particular instance. If this is not the case, it might be due to the following:

- Some switches may be temporarily disconnected and unreachable when the takeover message is sent.
- The takeover message might be lost on some links (however, the takeover messages are repeated to reduce this risk).

In both cases, you can correct the problem by issuing additional takeover messages.

For more information on configuring a takeover, see the [“Configuring a VTP Version 3 Takeover”](#) section on page 10-27.

VTP Version 3 Modes

The default mode for VTP is version 1, server mode. The off mode can be exited only after you configure a VTP domain name on the switch. The “domain discovery” that is used in VTP version 1 and VTP version 2 is not available in VTP version 3.

Switches running VTP version 3 have the following common characteristics:

- They accept only VTP packets from the same VTP domain.
- If they do not have a primary server, they accept the primary server that is associated with the first VTP database that they receive for any instance.
- They accept only a database with a higher revision number from their current primary server.
- If they have a password configured (whether hidden or not hidden), they accept only a new database or a takeover message if it contains the correct password.

VTP version 3 modes are described in the following sections:

- [Client Mode, page 10-18](#)
- [Server Mode, page 10-18](#)
- [Transparent and VTP Off Modes, page 10-19](#)

For more information on configuring modes, see the “[Changing VTP Version 3 Modes](#)” section on [page 10-23](#).

Client Mode

VTP version 3 clients are similar to VTP version 1 and VTP version 2 clients as follows:

- A VTP client accepts a VTP configuration from the network but cannot generate or alter the configuration.
- A VTP client stores the VTP configuration that it receives in RAM (not NVRAM). When a VTP client boots, it needs to reacquire the entire configuration that is propagated by VTP, including the identity of the primary server.
- A VTP client that cannot store the entire VTP configuration that is received in an instance to RAM, immediately transitions to transparent mode.

Server Mode

Primary and secondary servers are two types of servers that may exist on a VLAN or VTP instance in the VTP domain.

Secondary Server

When a switch is configured to be a server, it becomes a secondary server by default. As a secondary server, a VTP version 3 switch behaves as a client with the following exceptions:

- A secondary server immediately stores the information that is received through VTP version 3 in NVRAM. This NVRAM is part of the running configuration or startup configuration.
- At startup, a secondary server that has a configuration in NVRAM starts advertising the configuration. The main purpose of a VTP secondary server is to back up the configuration that is propagated over the network.
- Similar to a client, a VTP secondary server cannot modify the VTP configuration.
- A VTP server reverts to client mode if it cannot store the configuration in NVRAM.
- A VTP version 3 secondary server can issue a takeover to become a primary server.

Primary Server

The primary server can initiate or change the VTP configuration. To reach the primary server state, you must issue a successful takeover from the switch. The takeover is propagated to the entire domain. All other potential primary servers in the domain resign to secondary server mode to ensure that there is only one primary server in the VTP domain.

You only need the primary server when the VTP configuration for any instance needs to be modified. A VTP domain can operate with no active primary server because the secondary servers ensure persistence of the configuration over reloads. The primary server state is exited due to the following reasons:

- A switch reload.
- A high-availability switchover between the active and redundant supervisor engines.
- A takeover from another server.
- A change in the mode configuration.
- Any VTP domain configuration change (such as version, domain name, or domain password).

Transparent and VTP Off Modes

In VTP version 3, the transparent mode is specific to the instance. The off mode in VTP version 3 is similar to the previous VTP versions and is not specific to an instance. In both modes, you are allowed to configure locally the features that VTP is controlling. This configuration also appears in the running configuration (if applicable). The feature stores its local configuration in the same NVRAM block that is used by VTP. All NVRAM handling for the feature happens through VTP whether or not the switch is transparent to the feature. In VTP transparent mode, all VTP messages that are received by the switch are still flooded. In VTP off mode, the VTP messages are dropped on the trunks.

VTP Version 3 Databases

VTP version 1 and VTP version 2 are tied to VLAN information. VTP version 3 is designed to distribute any kind of configuration (referred to as a database) over a VTP domain.



Note

In software releases 8.1(x) and 8.2(x), the only supported database propagation is for the VLAN database. In software release 8.3(1), support is added to propagate the MST database.

These sections describe the VTP version 3 databases:

- [Valid Databases, page 10-19](#)
- [Database Revision Number, page 10-20](#)
- [Interaction with VTP Version 1 and VTP Version 2, page 10-20](#)
- [Limitations, page 10-21](#)

Valid Databases

A switch advertises a database only if it is valid. The only way to validate a database is to become the primary server. If a switch modifies a database that has been generated by a primary server (this situation is possible in off or transparent modes), the database is invalid. An invalid database is applied only locally on a switch and is overwritten by any database that is received on the network if the switch is a VTP client or server. Some examples of valid and invalid databases are as follows:

- When you move from VTP version 1 to VTP version 3, the VLAN database and MST database are not deleted but they are marked invalid because they have been generated by a VTP version 1 server, not by a VTP version 3 primary server.
- If you move a VTP version 3 server with a valid database to transparent mode, you can configure the VLAN database and MST database, but as soon as the database is modified, it becomes invalid. This situation prevents the switch from going back to server mode and advertising the database because the valid database that is received from the network overwrites the changes made while in transparent mode. If a server moves to transparent mode and then back to server mode with no changes to the database configuration, its database is still valid.
- If you modify a database on a primary server (such as a VLAN configuration), the database stays valid and is advertised to the rest of the domain. In any mode, when you configure a domain-related parameter (such as the domain name, VTP version, and the authentication method [password]), all the databases become invalidated. In addition to invalidating the databases, configuring a domain-related parameter also reverts a primary server to a secondary server.
- When you change a domain parameter, the switch is inserted into a new domain. To prevent the wrong database from accidentally being inserted into a VTP domain, you cannot insert a switch as a primary server into a new domain because it could potentially erase a valid configuration. Because it has an invalid database, a newly inserted switch in a domain immediately accepts the network configuration instead of erasing it.

Database Revision Number

Each VTP instance is associated with a database revision number. The database revision number is incremented when the value of the database that is covered by the advertised checksum is modified.

When a device receives a VTP advertisement from the same primary server for an instance in the same domain, the following occurs:

- If the database revision number in the advertisement is less than that of the receiving device, the advertisement is ignored and a summary advertisement with the current revision number is transmitted on the trunk on which the original advertisement was received.
- If the database revision number in the advertisement is the same as that of the receiving device, the following occurs:
 - If the checksum of the advertisement is exactly the same as the checksum of the current configuration known to the device, then no action is taken.
 - If the checksum of the advertisement is not exactly the same as the checksum of the current configuration known to the device, the device's configuration is unaffected, but the device indicates to the database manager that a configuration error condition has occurred.
- If the database revision number in the advertisement is greater than that of the receiving device, and the advertisement's checksum and configuration information match, the receiving switch requests the exact subset of databases for which it is not up to date.

The VTP advertisement is regenerated on each of the trunk ports of the device but not on the trunk port on which it was received.

Interaction with VTP Version 1 and VTP Version 2

VTP version 3 interacts with VTP version 1 and VTP version 2 switches as follows:

**Note**

You should configure VTP version 1 and VTP version 2 switches as clients to allow them to work properly with VTP version 3. See the [“Limitations” section on page 10-21](#) for more information.

- A VTP version 3 switch can detect VTP version 1 and VTP version 2 switches and send a scaled-down version of its database on a per-trunk basis in VTP version 2 format only. VTP version 1 switches move to VTP version 2 mode without any configuration assistance.
- A VTP version 3 switch never sends any VTP version 2 packets on a trunk unless it first receives a legacy VTP version 1 or VTP version 2 packet on the trunk. This situation forces legacy neighboring switches to keep advertising their presence on the link. If a VTP version 3 switch does not receive a legacy packet on a trunk for a certain period of time, it is considered to be a VTP version 3-only trunk and does not advertise a scaled-down version of the VLAN database or MST database on the trunk anymore.
- Even when advertising a VTP version 2 database on a trunk, VTP version 3 keeps sending VTP version 3 updates through the port. This situation allows two kinds of neighbors to coexist on the trunk.
- A VTP version 3 switch can modify reserved VLANs 1002–1005; however, these VLANs are set to their default in the scaled-down database in VTP version 2 format.
- A VTP version 3 switch never accepts a configuration from a VTP version 1 or VTP version 2 neighbor.

Limitations

The limitations of VTP version 3 are as follows:

- Two VTP version 3 regions can communicate only over a VTP version 1 and VTP version 2 region in transparent mode.
- Leaving a server in a VTP version 2 region so that it will receive its VTP information from a VTP version 3 region could cause a problem. If a configuration change occurs in the VTP version 1 and VTP version 2 region, the revision of the database may become higher than the one that is generated by the VTP version 3 region, and the updates from the VTP version 3 region may be ignored.

**Note**

We recommend that you set all switches in the VTP version 1 and VTP version 2 region to client and reset their revision number (do a reload or change the domain name back and forth).

- A VTP version 2 region that is connected to two different VTP version 3 regions may receive contradictory information and keep swapping its database to the VTP version 3 region that has the highest revision number at any given time. We do not recommend this type of configuration.
- Enabling VTP pruning on a VTP version 3 switch enables pruning only on the switch that you enable it on. VTP pruning is not propagated as it is with VTP version 1 and VTP version 2.

Default VTP Version 3 Configuration

[Table 10-2](#) shows the default VTP version 3 configuration.

Table 10-2 VTP Version 3 Default Configuration

Feature	Default Value
VTP domain name	Null
VTP mode	Server
VTP version 3 enable state	Version 1 is enabled
VTP password	None
VTP pruning	Disabled

Configuring VTP Version 3

These sections describe how to configure VTP version 3:

- [Enabling VTP Version 3, page 10-22](#)
- [Changing VTP Version 3 Modes, page 10-23](#)
- [Configuring VTP Version 3 Passwords, page 10-26](#)
- [Configuring a VTP Version 3 Takeover, page 10-27](#)
- [Disabling VTP Version 3 on a Per-Port Basis, page 10-28](#)
- [VTP Version 3 show Commands, page 10-29](#)

Enabling VTP Version 3

Use the `set vtp version version_number` command to specify the VTP version. By default, the VTP version is version 1 and the VTP mode is server mode. You must specify a domain before selecting a VTP version or VTP mode.

To enable VTP version 3, perform this task in privileged mode:

	Task	Command
Step 1	Enable VTP version 3 on the switch.	<code>set vtp version 3</code>
Step 2	Verify that VTP version 3 is enabled.	<code>show vtp domain</code>

This example shows how to enable VTP version 3 and verify the configuration:

```

Console> (enable) set vtp version 3
VTP version 3 cannot be enabled on a switch with No Domain.
Console> (enable) set vtp domain ENG
VTP domain ENG modified
Console> (enable) set vtp version 3
VTP version 3 Server/Client for VLANDB requires Reduced Mac Address feature to
be enabled (use "set spantree macreduction enable" command)
Console> (enable) set spantree macreduction enable
MAC address reduction enabled
Console> (enable) set vtp version 3
This command will enable VTP version 3 on this switch.
Do you want to continue (y/n) [n]? y
VTP3 domain ENG modified
Console> (enable) show vtp domain
    
```

```

Version      : running VTP3
Domain Name  : ENG
Notifications: disabled
Password    : configured
Switch ID   : 00d0.004c.1800

Feature      Mode          Revision  Primary ID  Primary Description
-----
VLAN         Server          0         0000.0000.0000
MST          Transparent
UNKNOWN      Transparent

Pruning      : disabled
VLANs prune eligible: 2-1000
Console> (enable)

```

Changing VTP Version 3 Modes



Note

For more information on VTP version modes, see the “[VTP Version 3 Modes](#)” section on page 10-17.

Each database is propagated by an instance of the VTP protocol. As these instances are independent, they can operate in different modes. The **set vtp mode** command allows you to set the mode for a particular VTP instance. The VTP instance is identified by the name of the feature to which it applies. The **set vtp mode** command has been extended to include a *feature* that you specify to identify the database to which the command applies. The **unknown** keyword allows you to configure the behavior of the switch databases that it cannot interpret. (These databases will be features handled by future extensions of VTP version 3.) If you enter the **set vtp mode transparent unknown** command, the packets for the unknown features are flooded through the switch. If you enter the **set vtp mode off unknown** command, the packets are dropped. The “unknown” feature can only be configured with off or transparent modes. The default mode is off for all databases. The mode of the VLAN database and MST database are preserved when VTP versions are changed.



Note

In software releases 8.1(x) and 8.2(x), the only supported database propagation is for the VLAN database; therefore, there are no “unknown” databases. In software release 8.3(1), support is added to propagate the MST database.

Configuring a VTP Version 3 Server

When a switch is in VTP version 3 server mode, you can change the VLAN configuration and have it propagate throughout the network. To configure the switch as a VTP version 3 server, perform this task in privileged mode:

	Task	Command
Step 1	Define the VTP domain name.	set vtp domain <i>name</i>
Step 2	Place the switch in VTP server mode.	set vtp mode server {vlan mst unknown}
Step 3	(Optional) Set a password for the VTP domain.	set vtp passwd <i>passwd</i>
Step 4	Verify the VTP configuration.	show vtp domain

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

```

Console> (enable) set vtp mode server vlan
Changing VTP mode for vlan feature

```

```
VTP3 domain map1 modified
Console> (enable) show vtp domain
Version      : running VTP3
Domain Name  : ENG                               Password  : configured
Notifications: disabled                         Switch ID : 00d0.004c.1800

Feature      Mode          Revision  Primary ID  Primary Description
-----
VLAN         Server         0         0000.0000.0000
MST          Transparent
UNKNOWN      Transparent

Pruning      : disabled
VLANs prune eligible: 2-1000
Console> (enable)
```

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

```
Console> (enable) set vtp mode server mst
Changing VTP mode for mst feature
VTP3 domain ENG modified
Console> (enable) show vtp domain
Version      : running VTP3
Domain Name  : ENG                               Password  : configured
Notifications: disabled                         Switch ID : 00d0.004c.1800

Feature      Mode          Revision  Primary ID  Primary Description
-----
VLAN         Server         0         0000.0000.0000
MST          Server         0         0000.0000.0000
UNKNOWN      Transparent

Pruning      : disabled
VLANs prune eligible: 2-1000
Console> (enable)
```

Configuring a VTP Version 3 Client

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

To configure the switch as a VTP version 3 client, perform this task in privileged mode:

	Task	Command
Step 1	Define the VTP domain name.	set vtp domain <i>name</i>
Step 2	Place the switch in VTP client mode.	set vtp mode client [vlan mst unknown]
Step 3	Verify the VTP configuration.	show vtp domain

This example shows how to configure the switch as a VTP version 3 VLAN client and verify the configuration:

```
Console> (enable) set vtp mode client vlan
Changing VTP mode for vlan feature
VTP3 domain ENG modified
Console> (enable) show vtp domain
Version      : running VTP3
Domain Name  : ENG                               Password  : configured
Notifications: disabled                         Switch ID : 00d0.004c.1800
```

```

Feature          Mode          Revision    Primary ID    Primary Description
-----
VLAN             Client        0           0000.0000.0000
MST              Server        0           0000.0000.0000
UNKNOWN         Transparent

Pruning          : disabled
VLANs prune eligible: 2-1000
Console> (enable)

```

Configuring VTP Version 3 Transparent Mode

When you configure the switch as VTP transparent, you disable VTP on the switch. A VTP transparent switch does not send VTP updates and does not act on VTP updates that are received from other switches.



Note

Network devices in VTP transparent mode do not send VTP join messages. On Catalyst 6500 series switches with trunk connections to network devices in VTP transparent mode, you should configure the VLANs that are used by the transparent-mode network devices or that need to be carried across trunks as pruning ineligible (use the **clear vtp pruneeligible** command).

To disable VTP on the switch, perform this task in privileged mode:

	Task	Command
Step 1	Disable VTP on the switch by configuring it for VTP transparent mode.	set vtp mode transparent [vlan mst unknown]
Step 2	Verify the VTP configuration.	show vtp domain

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

```

Console> (enable) set vtp mode transparent vlan
Changing VTP mode for vlan feature
VTP3 domain ENG modified
Console> (enable) show vtp domain
Version          : running VTP3
Domain Name     : ENG
Notifications   : disabled
Password        : configured
Switch ID       : 00d0.004c.1800

```

```

Feature          Mode          Revision    Primary ID    Primary Description
-----
VLAN             Transparent
MST              Server        0           0000.0000.0000
UNKNOWN         Transparent

Pruning          : disabled
VLANs prune eligible: 2-1000
Console> (enable)

```

Disabling VTP Using the Off Mode

When you disable VTP using the off mode, the switch behaves the same as in VTP transparent mode with the exception that VTP advertisements are not forwarded.

To disable VTP using the off mode, perform this task in privileged mode:

	Task	Command
Step 1	Disable VTP using the off mode.	set vtp mode off
Step 2	Verify the VTP configuration.	show vtp domain

This example shows how to disable VTP using the off mode:

```
Console> (enable) set vtp mode off
Changing VTP mode for all features
VTP3 domain server modified
```



Note

Because there is only the VLAN database in software releases 8.1(x) and 8.2(x), using the **set vtp mode off** command without specifying the **vlan** keyword results in the same configuration as using the **vlan** keyword. Note that in software release 8.3(1), support is added to propagate the MST database.

```
Console> (enable) show vtp domain
Version      : running VTP3
Domain Name  : ENG                               Password   : configured
Notifications: disabled                         Switch ID  : 00d0.004c.1800

Feature      Mode          Revision   Primary ID   Primary Description
-----
VLAN         Off
MST          Off
UNKNOWN     Transparent

Pruning      : disabled
VLANs prune eligible: 2-1000
Console> (enable)
```

Configuring VTP Version 3 Passwords



Note

For more information on passwords, see the [“VTP Version 3 Authentication” section on page 10-13](#).

In VTP version 3, you can hide the VTP password from the configuration by adding the **hidden** keyword to the password configuration. When you use the **hidden** keyword, the hexadecimal secret key that is generated from the password is shown in the configuration instead of the password in plain text. If you configure a password with the **hidden** keyword, you need to reenter the password to issue a takeover (for details on configuring a takeover, see the [“Configuring a VTP Version 3 Takeover” section on page 10-27](#)).

Two different formats of the **set vtp passwd** command can be shown in the configuration: A plain text password or an encrypted hexadecimal secret value. These two formats are exclusive; if you configure a plain text password, it replaces a current secret password, and similarly, if you paste a secret password into the configuration, the initial password is removed.

To configure VTP passwords, perform this task in privileged mode:

	Task	Command
Step 1	Configure a VTP password.	set vtp passwd <i>passwd</i> {hidden secret}
Step 2	Verify the VTP password.	show config

This example shows how to configure a VTP password and verify the configuration:

```

Console> (enable) set vtp passwd toto
Generating the secret associated to the password.
VTP3 domain server modified
Console> (enable) show config
.
.
.
set vtp passwd toto
.
.
.
Console> (enable) set vtp passwd toto hidden
Generating the secret associated to the password.
The VTP password will not be shown in the configuration.
VTP3 domain server modified

Console> (enable) show config
.
.
.
set vtp passwd 9fbdf74b43a2815037c1b33aa00445e2 secret
.
.
.
Console> (enable) set vtp passwd toto secret
VTP secret has to be 32 characters in length
Console> (enable)

```

This example shows how to copy the secret, hexadecimal value from the configuration, paste it into the command line, and verify the configuration:

```

Console> (enable) set vtp passwd 9fbdf74b43a2815037c1b33aa00445e2 secret
Setting secret.
VTP3 domain server modified
Console> (enable) show config
.
.
.
set vtp passwd 9fbdf74b43a2815037c1b33aa00445e2 secret
.
.
.

```

Configuring a VTP Version 3 Takeover



Note

For more information on takeovers, see the [“Reconfiguring a Partitioned VTP Domain”](#) section on page 10-16.

Use the **set vtp primary** [*feature*] [*force*] command to configure a takeover. A takeover allows a secondary server to become a primary server and propagates the primary server’s configuration to the entire VTP domain, removing any partitions if applicable.



Note

If a password was configured using the **hidden** keyword, you are prompted to reenter it.

If you do not specify the **force** keyword, the switch tries to discover some conflicting servers in the domain. Conflicting servers follow a different primary server than the one in the configuration of the local switch. You are prompted by the local switch for confirmation before proceeding with the takeover. The prompting is necessary because taking over the domain involves overwriting the configuration of any conflicting servers.

If you do not specify the optional *feature* argument, the local switch sends a takeover message for each database for which it is a secondary or a primary server. If you specify a database, the switch takes over only those databases that are associated with the specified feature.

To configure a takeover, perform this task in privileged mode:

	Task	Command
Step 1	Configure a takeover.	set vtp primary [<i>feature</i>] [force]
Step 2	Verify the takeover.	show vtp domain

This example shows how to configure a takeover from a secondary switch that has a hidden password configured and verify the configuration:

```

Console> (enable) set vtp primary force
Switch can become primary server for vlan feature only when configured as a server
Switch can become primary server for mst feature only when configured as a server
Console> (enable) set vtp mode server mst
Changing VTP mode for mst feature
VTP3 domain ENG modified
Console> (enable) set vtp mode server vlan
Changing VTP mode for vlan feature
VTP3 domain ENG modified
Console> (enable) set vtp primary force
This switch is becoming primary server for feature vlan.
This switch is becoming primary server for feature mst.
Do you want to continue (y/n) [n]? y
Console> (enable) show vtp domain
Version          : running VTP3
Domain Name     : ENG                               Password  : configured
Notifications: disabled                           Switch ID : 00d0.004c.1800

Feature          Mode          Revision    Primary ID    Primary Description
-----
VLAN             Primary Server 1    00d0.004c.1800
MST              Primary Server 1    00d0.004c.1800
UNKNOWN         Transparent

Pruning          : disabled
VLANs prune eligible: 2-1000
Console> (enable)
    
```

Disabling VTP Version 3 on a Per-Port Basis



Note

For more information on disabling VTP version 3 on a per-port basis, see the [“VTP Version 3 Per-Port Configuration”](#) section on page 10-14.

Use the **set port vtp *mod/port* {enable | disable}** command to enable or disable all VTP interaction on a per-port basis. This capability might be used on trunks leading to nontrusted hosts. When a port is disabled, no VTP packets are sent on the port, and any VTP packets that are received on the port are dropped. By default, VTP is enabled and advertisements are received and sent on all trunks.

To disable VTP on a per-port basis, perform this task in privileged mode:

	Task	Command
Step 1	Disable VTP on a per-port basis.	set port vtp <i>mod/port</i> {enable disable}
Step 2	Verify the change.	show port vtp

This example shows how to disable VTP on a per-port basis and verify the configuration:

```

Console> (enable) set port vtp 3/1-2 disable
VTP is disabled on ports 3/1-2.
Console> (enable) show port vtp 3
Port      VTP Status
-----
3/1      disabled
3/2      disabled
3/3      enabled
3/4      enabled
Console> (enable)

```

VTP Version 3 show Commands

Use the **show vtp {conflicts | devices | domain | statistics}** command to show other **devices** in the domain or devices in the domain with conflicting (**conflicts**) configurations. Use the **domain** keyword to display information that is specific to the VTP domain. Use the **statistics** keyword to display VTP statistics. Switches in transparent or off mode are not part of the VTP domain and do not respond to requests. In addition, the clients or servers that do not have a valid database do not respond to requests.

