Configuring VTP

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for VTP

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

VTP is designed to work in an environment where updates are made on a single controller and are sent through VTP to other controllers in the domain. It does not work well in a situation where multiple updates to the VLAN database occur simultaneously on controllers in the same domain, which would result in an inconsistency in the VLAN database.

The controller supports a total of 4094 VLANs. However, the number of configured features affects the usage of the controller hardware. If the controller is notified by VTP of a new VLAN and the controller is already using the maximum available hardware resources, it sends a message that there are not enough hardware resources available and shuts down the VLAN. The output of the **show vlan** user EXEC command shows the VLAN in a suspended state.

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

Related Topics

VTP Advertisements, on page 4

Adding a VTP Client Controller to a VTP Domain , on page 19

VTP Domain, on page 3

VTP Modes, on page 3

Restrictions for VTP

The following are restrictions for a VTP:

- You cannot have a controller stack containing a mix of Catalyst 3850 and Catalyst 3650 switches.

Caution Before adding a VTP client controller to a VTP domain, always verify that its VTP configuration revision number is lower than the configuration revision number of the other controllers in the VTP domain. Controllers in a VTP domain always use the VLAN configuration of the controller with the highest VTP configuration revision number. If you add a controller that has a revision number higher than the revision number in the VTP domain, it can erase all VLAN information from the VTP server and VTP domain.

Information About VTP

VTP

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

VTP Domain

A VTP domain (also called a VLAN management domain) consists of one controller or several interconnected controllers or controller stacks under the same administrative responsibility sharing the same VTP domain name. A controller can be in only one VTP domain. You make global VLAN configuration changes for the domain.

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

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

When you make a change to the VLAN configuration on a VTP server, the change is propagated to all controllers in the VTP domain. VTP advertisements are sent over all IEEE trunk connections, including IEEE 802.1Q. VTP dynamically maps VLANs with unique names and internal index associates across multiple LAN types. Mapping eliminates excessive device administration required from network administrators.

If you configure a controller for VTP transparent mode, you can create and modify VLANs, but the changes are not sent to other controllers in the domain, and they affect only the individual controller. However, configuration changes made when the controller is in this mode are saved in the controller running configuration and can be saved to the controller startup configuration file.

Related Topics

Adding a VTP Client Controller to a VTP Domain , on page 19

Prerequisites for VTP, on page 1

VTP Modes

Table 1: VTP Modes

VTP Mode	Description
VTP server	In VTP server mode, you can create, modify, and delete VLANs, and specify other configuration parameters (such as the VTP version) for the entire VTP domain. VTP servers advertise their VLAN configurations to other controllers in the same VTP domain and synchronize their VLAN configurations with other controllers based on advertisements received over trunk links. VTP server is the default mode. In VTP server mode, VLAN configurations are saved in NVRAM. If the controller detects a failure while writing a configuration to NVRAM, VTP mode automatically changes from server mode to client mode. If this happens, the controller cannot be returned to VTP server mode until the NVRAM is functioning.

VTP Mode	Description
VTP client	A VTP client functions like a VTP server and transmits and receives VTP updates on its trunks, but you cannot create, change, or delete VLANs on a VTP client. VLANs are configured on another controller in the domain that is in server mode. In VTP versions 1 and 2 in VTP client mode, VLAN configurations are not saved in NVRAM. In VTP version 3, VLAN configurations are saved in NVRAM in client mode.
VTP transparent	VTP transparent controllers do not participate in VTP. A VTP transparent controller does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. However, in VTP version 2 or version 3, transparent controllers do forward VTP advertisements that they receive from other controllers through their trunk interfaces. You can create, modify, and delete VLANs on a controller in VTP transparent mode. When the controller is in VTP transparent mode, the VTP and VLAN configurations are saved in NVRAM, but they are not advertised to other controllers. In this mode, VTP mode and domain name are saved in the controller running configuration, and you can save this information in the controller startup configuration file by using the **copy running-config startup-config** privileged EXEC command.
VTP off	A controller in VTP off mode functions in the same manner as a VTP transparent controller, except that it does not forward VTP advertisements on trunks.

Related Topics

Prerequisites for VTP, on page 1
Configuring VTP Mode , on page 10

VTP Advertisements

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

VTP advertisements distribute this global domain information:

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

VTP advertisements distribute this VLAN information for each configured VLAN:

- VLAN IDs (including IEEE 802.1Q)
- VLAN name

- VLAN type
- VLAN state
- Additional VLAN configuration information specific to the VLAN type

In VTP version 3, VTP advertisements also include the primary server ID, an instance number, and a start index.

Related Topics

Prerequisites for VTP, on page 1

VTP Version 2

If you use VTP in your network, you must decide which version of VTP to use. By default, VTP operates in version 1.

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

- Token Ring support—VTP version 2 supports Token Ring Bridge Relay Function (TrBRF) and Token Ring Concentrator Relay Function (TrCRF) VLANs.
- Unrecognized Type-Length-Value (TLV) support—A VTP server or client propagates configuration changes to its other trunks, even for TLVs it is not able to parse. The unrecognized TLV is saved in NVRAM when the controller is operating in VTP server mode.
- Version-Dependent Transparent Mode—In VTP version 1, a VTP transparent controller inspects VTP messages for the domain name and version and forwards a message only if the version and domain name match. Although VTP version 2 supports only one domain, a VTP version 2 transparent controller forwards a message only when the domain name matches.
- 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 MD5 digest on a received VTP message is correct, its information is accepted.

Related Topics

Enabling the VTP Version , on page 15

VTP Version 3

VTP version 3 supports these features that are not supported in version 1 or version 2:

- Enhanced authentication—You can configure the authentication as **hidden** or **secret**. When **hidden**, the secret key from the password string is saved in the VLAN database file, but it does not appear in plain text in the configuration. Instead, the key associated with the password is saved in hexadecimal format in the running configuration. You must reenter the password if you enter a takeover command in the domain. When you enter the **secret** keyword, you can directly configure the password secret key.
- Support for extended range VLAN (VLANs 1006 to 4094) database propagation—VTP versions 1 and 2 propagate only VLANs 1 to 1005.

Note VTP pruning still applies only to VLANs 1 to 1005, and VLANs 1002 to 1005 are still reserved and cannot be modified.

- Support for any database in a domain—In addition to propagating VTP information, version 3 can propagate Multiple Spanning Tree (MST) protocol database information. A separate instance of the VTP protocol runs for each application that uses VTP.
- VTP primary server and VTP secondary servers—A VTP primary server updates the database information and sends updates that are honored by all devices in the system. A VTP secondary server can only back up the updated VTP configurations received from the primary server to its NVRAM.

  By default, all devices come up as secondary servers. You can enter the **vtp primary** privileged EXEC command to specify a primary server. Primary server status is only needed for database updates when the administrator issues a takeover message in the domain. You can have a working VTP domain without any primary servers. Primary server status is lost if the device reloads or domain parameters change, even when a password is configured on the controller.
- The option to turn VTP on or off on a per-trunk (per-port) basis—You can enable or disable VTP per port by entering the [**no**] **vtp** interface configuration command. When you disable VTP on trunking ports, all VTP instances for that port are disabled. You cannot set VTP to *off* for the MST database and *on* for the VLAN database on the same port.

  When you globally set VTP mode to off, it applies to all the trunking ports in the system. However, you can specify on or off on a per-VTP instance basis. For example, you can configure the controller as a VTP server for the VLAN database but with VTP *off* for the MST database.

Related Topics

Enabling the VTP Version , on page 15

VTP Pruning

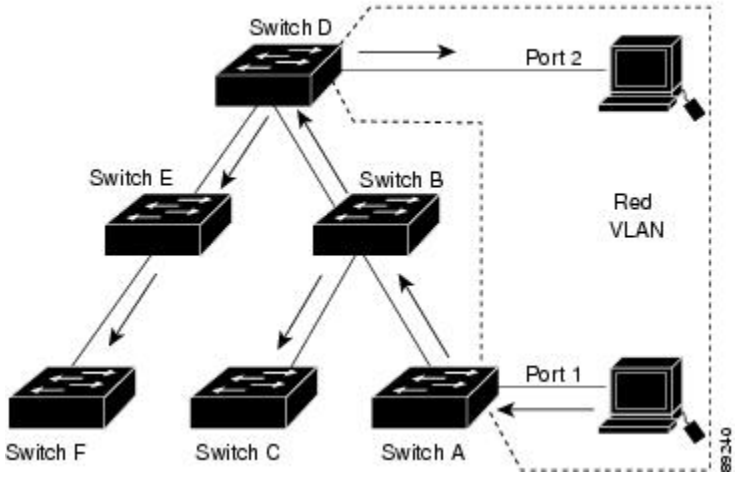
VTP pruning increases network available bandwidth by restricting flooded traffic to those trunk links that the traffic must use to reach the destination devices. Without VTP pruning, a controller floods broadcast, multicast, and unknown unicast traffic across all trunk links within a VTP domain even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

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

VTP pruning is disabled in the switched network. Port 1 on Controller A and Port 2 on Controller D are assigned to the Red VLAN. If a broadcast is sent from the host connected to Controller A, Controller A floods

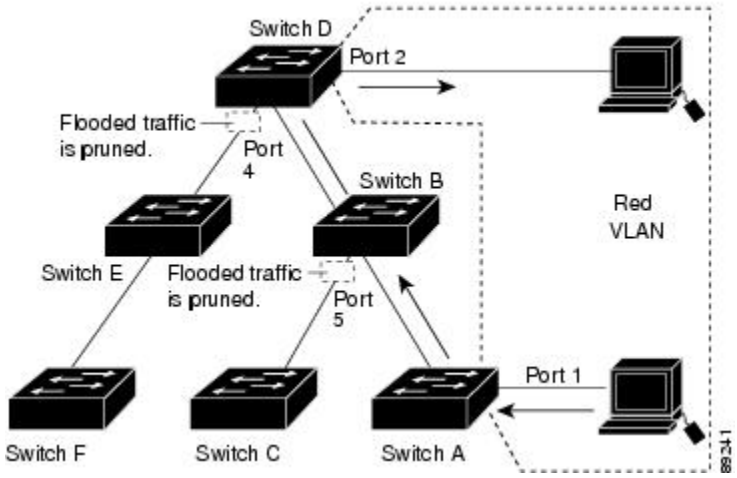
the broadcast and every controller in the network receives it, even though Controllers C, E, and F have no ports in the Red VLAN.

Figure 1: Flooding Traffic without VTP Pruning



VTP pruning is enabled in the switched network. The broadcast traffic from Controller A is not forwarded to Controllers C, E, and F because traffic for the Red VLAN has been pruned on the links shown (Port 5 on Controller B and Port 4 on Controller D).

Figure 2: Optimized Flooded Traffic VTP Pruning



With VTP versions 1 and 2, when you enable pruning on the VTP server, it is enabled for the entire VTP domain. In VTP version 3, you must manually enable pruning on each controller in the domain. Making VLANs pruning-eligible or pruning-ineligible affects pruning eligibility for those VLANs on that trunk only (not on all controllers in the VTP domain).

VTP pruning takes effect several seconds after you enable it. VTP pruning does not prune traffic from VLANs that are pruning-ineligible. VLAN 1 and VLANs 1002 to 1005 are always pruning-ineligible; traffic from these VLANs cannot be pruned. Extended-range VLANs (VLAN IDs higher than 1005) are also pruning-ineligible.

Related Topics

Enabling VTP Pruning , on page 16

VTP Configuration Guidelines

VTP Configuration Requirements

When you configure VTP, you must configure a trunk port so that the controller can send and receive VTP advertisements to and from other controllers in the domain.

VTP Settings

The VTP information is saved in the VTP VLAN database. When VTP mode is transparent, the VTP domain name and mode are also saved in the controller running configuration file, and you can save it in the controller startup configuration file by entering the **copy running-config startup-config** privileged EXEC command. You must use this command if you want to save VTP mode as transparent, even if the controller resets.

When you save VTP information in the controller startup configuration file and reboot the controller, the controller configuration is selected as follows:

- If the VTP mode is transparent in the startup configuration and the VLAN database and the VTP domain name from the VLAN database matches that in the startup configuration file, the VLAN database is ignored (cleared), and the VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.
- If the VTP mode or domain name in the startup configuration do not match the VLAN database, the domain name and VTP mode and configuration for VLAN IDs 1 to 1005 use the VLAN database information.

Related Topics

Configuring VTP on a Per-Port Basis , on page 18

Configuring a VTP Version 3 Primary Server , on page 14

Domain Names for Configuring VTP

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

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

Caution Do not configure a VTP domain if all controllers are operating in VTP client mode. If you configure the domain, it is impossible to make changes to the VLAN configuration of that domain. Make sure that you configure at least one controller in the VTP domain for VTP server mode.

Related Topics

Adding a VTP Client Controller to a VTP Domain , on page 19

Passwords for the VTP Domain

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

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

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

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

Related Topics

Configuring a VTP Version 3 Password , on page 12

Example: Configuring a Switch as the Primary Server, on page 22

VTP Version

Follow these guidelines when deciding which VTP version to implement:

- All controllers in a VTP domain must have the same domain name, but they do not need to run the same VTP version.
- A VTP version 2-capable controller can operate in the same VTP domain as a controller running VTP version 1 if version 2 is disabled on the version 2-capable controller (version 2 is disabled by default).
- If a controller running VTP version 1, but capable of running VTP version 2, receives VTP version 3 advertisements, it automatically moves to VTP version 2.
- If a controller running VTP version 3 is connected to a controller running VTP version 1, the VTP version 1 controller moves to VTP version 2, and the VTP version 3 controller sends scaled-down versions of the VTP packets so that the VTP version 2 controller can update its database.
- A controller running VTP version 3 cannot move to version 1 or 2 if it has extended VLANs.

- Do not enable VTP version 2 on a controller unless all of the controllers in the same VTP domain are version-2-capable. When you enable version 2 on a controller, all of the version-2-capable controllers in the domain enable version 2. If there is a version 1-only controller, it does not exchange VTP information with controllers that have version 2 enabled.
- Cisco recommends placing VTP version 1 and 2 controllers at the edge of the network because they do not forward VTP version 3 advertisements.
- If there are TrBRF and TrCRF Token Ring networks in your environment, you must enable VTP version 2 or version 3 for Token Ring VLAN switching to function properly. To run Token Ring and Token Ring-Net, disable VTP version 2.
- VTP version 1 and version 2 do not propagate configuration information for extended range VLANs (VLANs 1006 to 4094). You must configure these VLANs manually on each device. VTP version 3 supports extended-range VLANs and support for extended range VLAN database propagation.
- When a VTP version 3 device 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 VTP version 2 format. A VTP version 3 device does not send VTP version 2-formatted packets on a trunk unless it first receives VTP version 2 packets on that trunk port.
- 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 both kinds of neighbors to coexist on the same trunk.
- A VTP version 3 device does not accept configuration information from a VTP version 2 or version 1 device.
- Two VTP version 3 regions can only communicate in transparent mode over a VTP version 1 or version 2 region.
- Devices that are only VTP version 1 capable cannot interoperate with VTP version 3 devices.
- VTP version 1 and version 2 do not propagate configuration information for extended range VLANs (VLANs 1006 to 4094). You must manually configure these VLANs on each device.

Related Topics

Enabling the VTP Version , on page 15

How to Configure VTP

Configuring VTP Mode

You can configure VTP mode as one of these:

- VTP server mode—In VTP server mode, you can change the VLAN configuration and have it propagated throughout the network.
- VTP client mode—In VTP client mode, you cannot change its VLAN configuration. The client controller receives VTP updates from a VTP server in the VTP domain and then modifies its configuration accordingly.

- VTP transparent mode—In VTP transparent mode, VTP is disabled on the controller. The controller does not send VTP updates and does not act on VTP updates received from other controller. However, a VTP transparent controller running VTP version 2 does forward received VTP advertisements on its trunk links.
- VTP off mode—VTP off mode is the same as VTP transparent mode except that VTP advertisements are not forwarded.

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vtp domain** *domain-name*
4. **vtp mode** {**client** | **server** | **transparent** | **off**} {**vlan** | **mst** | **unknown**}
5. **vtp password** *password*
6. **end**
7. **show vtp status**
8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Controller> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Controller# configure terminal`	Enters the global configuration mode.
Step 3	**vtp domain** *domain-name* **Example:** `Controller(config)# vtp domain eng_group`	Configures the VTP administrative-domain name. The name can be 1 to 32 characters. All controllers operating in VTP server or client mode under the same administrative responsibility must be configured with the same domain name. This command is optional for modes other than server mode. VTP server mode requires a domain name. If the controller has a trunk connection to a VTP domain, the controller learns the domain name from the VTP server in the domain. You should configure the VTP domain before configuring other VTP parameters.

	Command or Action	Purpose
		Note
Step 4	**vtp mode** {**client** | **server** | **transparent** | **off**} {**vlan** | **mst** | **unknown**} **Example:** `Controller(config)# vtp mode server`	Configures the controller for VTP mode (client, server, transparent, or off). • **vlan—**The VLAN database is the default if none are configured. • **mst—**The multiple spanning tree (MST) database. • **unknown—**An unknown database type.
Step 5	**vtp password** *password* **Example:** `Controller(config)# vtp password mypassword`	(Optional) Sets the password for the VTP domain. The password can be 8 to 64 characters. If you configure a VTP password, the VTP domain does not function properly if you do not assign the same password to each controller in the domain.
Step 6	**end** **Example:** `Controller(config)# end`	Returns to privileged EXEC mode.
Step 7	**show vtp status** **Example:** `Controller# show vtp status`	Verifies your entries in the *VTP Operating Mode* and the *VTP Domain Name* fields of the display.
Step 8	**copy running-config startup-config** **Example:** `Controller# copy running-config startup-config`	(Optional) Saves the configuration in the startup configuration file. Only VTP mode and domain name are saved in the controller running configuration and can be copied to the startup configuration file.

Related Topics

VTP Modes, on page 3

Configuring a VTP Version 3 Password

You can configure a VTP version 3 password on the controller.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vtp password** *password* [**hidden** | **secret**]
4. **end**
5. **show vtp password**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Controller> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Controller# configure terminal`	Enters the global configuration mode.
Step 3	**vtp password** *password* [**hidden**	**secret**] **Example:** `Controller(config)# vtp password mypassword hidden`	(Optional) Sets the password for the VTP domain. The password can be 8 to 64 characters. • (Optional) **hidden—**Saves the secret key generated from the password string in the nvram:vlan.dat file. If you configure a takeover by configuring a VTP primary server, you are prompted to reenter the password. • (Optional) **secret—**Directly configures the password. The secret password must contain 32 hexadecimal characters.
Step 4	**end** **Example:** `Controller(config)# end`	Returns to privileged EXEC mode.
Step 5	**show vtp password** **Example:** `Controller# show vtp password`	Verifies your entries. The output appears like this: VTP password: 89914640C8D90868B6A0D8103847A733

	Command or Action	Purpose
Step 6	**copy running-config startup-config** **Example:** `Controller# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

Passwords for the VTP Domain, on page 9
Example: Configuring a Switch as the Primary Server, on page 22

Configuring a VTP Version 3 Primary Server

When you configure a VTP server as a VTP primary server, the takeover operation starts.

SUMMARY STEPS

1. **vtp primary** [**vlan** | **mst**] [**force**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**vtp primary** [**vlan**	**mst**] [**force**] **Example:** `Controller# vtp primary vlan force`	Changes the operational state of a controller from a secondary server (the default) to a primary server and advertises the configuration to the domain. If the controller password is configured as **hidden**, you are prompted to reenter the password. • (Optional) **vlan**—Selects the VLAN database as the takeover feature. This is the default. • (Optional) **mst**—Selects the multiple spanning tree (MST) database as the takeover feature. • (Optional) **force**—Overwrites the configuration of any conflicting servers. If you do not enter **force**, you are prompted for confirmation before the takeover.

Related Topics

VTP Settings, on page 8

Enabling the VTP Version

VTP version 2 and version 3 are disabled by default.

- When you enable VTP version 2 on a controller , every VTP version 2-capable controller in the VTP domain enables version 2. To enable VTP version 3, you must manually configure it on each controller .
- With VTP versions 1 and 2, you can configure the version only on controllers in VTP server or transparent mode. If a controller is running VTP version 3, you can change to version 2 when the controller is in client mode if no extended VLANs exist, and no hidden password was configured.

  Caution VTP version 1 and VTP version 2 are not interoperable on controllers in the same VTP domain. Do not enable VTP version 2 unless every controller in the VTP domain supports version 2.

- In TrCRF and TrBRF Token Ring environments, you must enable VTP version 2 or VTP version 3 for Token Ring VLAN switching to function properly. For Token Ring and Token Ring-Net media, disable VTP version 2.
- **Caution** In VTP version 3, both the primary and secondary servers can exist on an instance in the domain.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vtp version** {**1** | **2** | **3**}
4. **end**
5. **show vtp status**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Controller> enable`	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Controller# configure terminal`	Enters the global configuration mode.
Step 3	**vtp version** {**1** | **2** | **3**} **Example:** `Controller(config)# vtp version 2`	Enables the VTP version on the controller. The default is VTP version 1.
Step 4	**end** **Example:** `Controller(config)# end`	Returns to privileged EXEC mode.
Step 5	**show vtp status** **Example:** `Controller# show vtp status`	Verifies that the configured VTP version is enabled.
Step 6	**copy running-config startup-config** **Example:** `Controller# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

VTP Version, on page 9
VTP Version 2, on page 5
VTP Version 3, on page 5

Enabling VTP Pruning

Before You Begin

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

- Turn off VTP pruning in the entire network.

- Turn off VTP pruning by making all VLANs on the trunk of the controller upstream to the VTP transparent controller pruning ineligible.

To configure VTP pruning on an interface, use the **switchport trunk pruning vlan** interface configuration command. VTP pruning operates when an interface is trunking. You can set VLAN pruning-eligibility, whether or not VTP pruning is enabled for the VTP domain, whether or not any given VLAN exists, and whether or not the interface is currently trunking.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vtp pruning**
4. **end**
5. **show vtp status**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Controller> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Controller# configure terminal`	Enters the global configuration mode.
Step 3	**vtp pruning** **Example:** `Controller(config)# vtp pruning`	Enables pruning in the VTP administrative domain. By default, pruning is disabled. You need to enable pruning on only one controller in VTP server mode.
Step 4	**end** **Example:** `Controller(config)# end`	Returns to privileged EXEC mode.
Step 5	**show vtp status** **Example:** `Controller# show vtp status`	Verifies your entries in the *VTP Pruning Mode* field of the display.

Related Topics

VTP Pruning, on page 6

Configuring VTP on a Per-Port Basis

With VTP version 3, you can enable or disable VTP on a per-port basis. You can enable VTP only on ports that are in trunk mode. Incoming and outgoing VTP traffic are blocked, not forwarded.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **vtp**
5. **end**
6. **show running-config interface** *interface-id*
7. **show vtp status**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Controller> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Controller# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Controller(config)# interface gigabitethernet1/0/1`	Identifies an interface, and enters interface configuration mode.

	Command or Action	Purpose
Step 4	**vtp** **Example:** `Controller(config)# vtp`	Enables VTP on the specified port.
Step 5	**end** **Example:** `Controller(config)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config interface** *interface-id* **Example:** `Controller# show running-config interface gigabitethernet1/0/1`	Verifies the change to the port.
Step 7	**show vtp status** **Example:** `Controller# show vtp status`	Verifies the configuration.

Related Topics

VTP Settings, on page 8

Adding a VTP Client Controller to a VTP Domain

Follow these steps to verify and reset the VTP configuration revision number on a controller *before* adding it to a VTP domain.

Before You Begin

Before adding a VTP client to a VTP domain, always verify that its VTP configuration revision number is *lower* than the configuration revision number of the other controllers in the VTP domain. Controllers in a VTP domain always use the VLAN configuration of the controller with the highest VTP configuration revision number. With VTP versions 1 and 2, adding a controller that has a revision number higher than the revision number in the VTP domain can erase all VLAN information from the VTP server and VTP domain. With VTP version 3, the VLAN information is not erased.

You can use the **vtp mode transparent** global configuration command to disable VTP on the controller and then to change its VLAN information without affecting the other controllers in the VTP domain.

SUMMARY STEPS

1. **enable**
2. **show vtp status**
3. **configure terminal**
4. **vtp domain** *domain-name*
5. **end**
6. **show vtp status**
7. **configure terminal**
8. **vtp domain** *domain-name*
9. **end**
10. **show vtp status**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Controller> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**show vtp status** **Example:** `Controller# show vtp status`	Checks the VTP configuration revision number. If the number is 0, add the controller to the VTP domain. If the number is greater than 0, follow these substeps: • Write down the domain name. • Write down the configuration revision number. • Continue with the next steps to reset the controller configuration revision number.
Step 3	**configure terminal** **Example:** `Controller# configure terminal`	Enters the global configuration mode.
Step 4	**vtp domain** *domain-name* **Example:** `Controller(config)# vtp domain domain123`	Changes the domain name from the original one displayed in Step 1 to a new name.

	Command or Action	Purpose
Step 5	**end** **Example:** `Controller(config)# end`	Returns to privileged EXEC mode. The VLAN information on the controller is updated and the configuration revision number is reset to 0.
Step 6	**show vtp status** **Example:** `Controller# show vtp status`	Verifies that the configuration revision number has been reset to 0.
Step 7	**configure terminal** **Example:** `Controller# configure terminal`	Enters global configuration mode.
Step 8	**vtp domain** *domain-name* **Example:** `Controller(config)# vtp domain domain012`	Enters the original domain name on the controller
Step 9	**end** **Example:** `Controller(config)# end`	Returns to privileged EXEC mode. The VLAN information on the controller is updated.
Step 10	**show vtp status** **Example:** `Controller# show vtp status`	(Optional) Verifies that the domain name is the same as in Step 1 and that the configuration revision number is 0.

Related Topics

VTP Domain, on page 3
Prerequisites for VTP, on page 1
Domain Names for Configuring VTP, on page 8

Monitoring VTP

This section describes commands used to display and monitor the VTP configuration.

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

Table 2: VTP Monitoring Commands

Command	Purpose
show vtp counters	Displays counters about VTP messages that have been sent and received.
show vtp devices [**conflict**]	Displays information about all VTP version 3 devices in the domain. Conflicts are VTP version 3 devices with conflicting primary servers. The **show vtp devices** command does not display information when the controller is in transparent or off mode.
show vtp interface [*interface-id*]	Displays VTP status and configuration for all interfaces or the specified interface.
show vtp password	Displays the VTP password. The form of the password displayed depends on whether or not the **hidden** keyword was entered and if encryption is enabled on the controller.
show vtp status	Displays the VTP controller configuration information.

Configuration Examples for VTP

Example: Configuring a Switch as the Primary Server

This example shows how to configure a controller as the primary server for the VLAN database (the default) when a hidden or secret password was configured:

```
Controller# vtp primary vlan
Enter VTP password: mypassword
This switch is becoming Primary server for vlan feature in the VTP  domain

VTP Database Conf Switch ID      Primary Server Revision System Name
------------ ---- --------------- -------------- -------- --------------------
VLANDB       Yes  00d0.00b8.1400=00d0.00b8.1400 1        stp7

Do you want to continue (y/n) [n]? y
```

Related Topics

Configuring a VTP Version 3 Password , on page 12
Passwords for the VTP Domain, on page 9

Where to Go Next

After configuring VTP, you can configure the following:

- VLANs
- VLAN groups
- VLAN trunking

Additional References

Standards and RFCs

Standard/RFC	Title
RFC 1573	Evolution of the Interfaces Group of MIB-II
RFC 1757	Remote Network Monitoring Management
RFC 2021	SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2

MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information for VTP

Release	Modification
Cisco IOS XE 3.2SECisco IOS XE 3.2SE	This feature was introduced.