Configuring VTP

This chapter describes how to configure VLAN Trunking Protocol (VTP) and VTP pruning on Cisco NX-OS devices.

This chapter includes the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your 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 "New and Changed Information"chapter or the Feature History table in this chapter.

Information About VTP

Beginning with Cisco NX-OS Release 5.1(1), VTP and VTP pruning are supported for VTP version 1 and 2. Before Release 5.1(1), only VTP transparent mode was supported.

Note Beginning with Cisco NX-OS Release 5.1(1), you can configure VLANs without actually creating the VLANs. For more details, see Configuring a VLAN Before Creating the VLAN.

VTP

VTP is a Layer 2 messaging protocol that maintains VLAN consistency by managing the addition, deletion, and renaming of VLANs within a VTP domain. A VTP domain is made up of one or more network devices that share the same VTP domain name and that are connected with trunk interfaces. Each network device can be in only one VTP domain.

Layer 2 trunk interfaces, Layer 2 port channels, and virtual port channels (vPCs) support VTP functionality.

The VTP is disabled by default on the device. You can enable and configure VTP using the command-line interface (CLI). When VTP is disabled, the device does not relay any VTP protocol packets.

Note Before Release 5.1(1), VTP worked only in transparent mode in the Cisco Nexus 7000 Series devices, allowing you to extend a VTP domain across the device.

When the device is in the VTP transparent mode, the device relays all VTP protocol packets that it receives on a trunk port to all other trunk ports. When you create or modify a VLAN that is in VTP transparent mode, those VLAN changes affect only the local device. A VTP transparent network device does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements.

Note VLAN 1 is required on all trunk ports used for switch interconnects if VTP is supported in the network. Before 7.2(0)D1(1), disabling VLAN 1 from any of these ports prevents VTP from functioning properly.

If you enable VTP, you must configure either version 1 or version 2. If you are using VTP in a Token Ring environment, you must use version 2.

VTP Overview

VTP allows each router or LAN device to transmit advertisements in frames on its trunk ports. These frames are sent to a multicast address where they can be received by all neighboring devices. They are not forwarded by normal bridging procedures. An advertisement lists the sending device's VTP management domain, its configuration revision number, the VLANs which it knows about, and certain parameters for each known VLAN. By hearing these advertisements, all devices in the same management domain learn about any new VLANs that are configured in the transmitting device. This process allows you to create and configure a new VLAN only on one device in the management domain, and then that information is automatically learned by all the other devices in the same management domain.

Once a device learns about a VLAN, the device receives all frames on that VLAN from any trunk port by default, and if appropriate, forwards them to each of its other trunk ports, if any. This process prevents unnecessary VLAN traffic from being sent to a device. An extension of VTP called VTP pruning has been defined to limit the scope of broadcast traffic and save bandwidth. Beginning with Release 5.1(1), the Cisco NX-OS software supports VTP pruning.

VTP also publishes information about the domain and the mode in a shared local database that can be read by other processes such as Cisco Discovery Protocol (CDP).

VTP Modes

Beginning with Release 5.1(1), VTP is supported in these modes:

- Transparent—Allows you to relay all VTP protocol packets that it receives on a trunk port to all other trunk ports. When you create or modify a VLAN that is in VTP transparent mode, those VLAN changes affect only the local device. A VTP transparent network device does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. You cannot configure VLANs 1002 to 1005 in VTP client/server mode because these VLANs are reserved for Token Ring.
- Server— Allows you to create, remove, and modify VLANs over the entire network. You can set other configuration options like the VTP version and also turn on or off 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 messages received over trunk links. Beginning with Release 5.1(1), the server mode is the default mode. The VLAN information is stored on the bootflash and is not erased after a reboot.
- Client—VTP clients behave the same way as VTP servers, but you cannot create, change, or delete VLANs on a VTP client.
- Off— Behaves similarly to the transparent mode but does not forward any VTP packets. The off mode allows you to monitor VLANs by using the CISCO-VTP-MIB without having to run VTP. On Cisco Nexus 7000 Series devices, because VTP is a conditional service, its MIB is loaded only when the corresponding feature is enabled. The CISCO-VTP-MIB does not follow this convention. It is loaded by the VLAN manager and will always return the correct values whether the VTP process is enabled or disabled.

Beginning with Cisco NX-OS Release 6.1(1), if VTP is in transparent or in off mode, you can configure VLAN long names of up to 128 characters. If VTP is in client or server mode, you cannot enable VLAN long-names. For more details, see the Configuring VLANs chapter.

VTP Per Interface

VTP allows you to enable or disable the VTP protocol on a per-port basis to control the VTP traffic. When a trunk is connected to a switch or end device, it drops incoming VTP packets and prevents VTP advertisements on this particular trunk. By default, VTP is enabled on all the switch ports.

VTP Pruning

The VLAN architecture requires all flooded traffic for a VLAN to be sent across a trunk port even if it leads to switches that have no devices that are active in the VLAN. This method leads to wasted network bandwidth.

VTP pruning optimizes the usage of network bandwidth by restricting the flooded traffic to only those trunk ports that can reach all the active network devices. When this protocol is in use, a trunk port does not receive the flooded traffic that is meant for a certain VLAN unless an appropriate join message is received.

A join message is defined as a new message type in addition to the ones already supported by version 1 of VTP. A VTP implementation indicates that it supports this extension by appending a special TLV at the end of the summary advertisement messages that it generates. In VTP transparent mode, VTP relays all VTP packets, and pruning requires that the switch processes TLVs in the VTP summary packets. You cannot use pruning in VTP transparent mode.

VTP Pruning and Spanning Tree Protocol

VTP maintains a list of trunk ports in the Spanning Tree Protocol (STP) forwarding state by querying STP at bootup and listening to the notifications that are generated by STP.

VTP sets a trunk port into the pruned or joined state by interacting with STP. STP notifies VTP when a trunk port goes to the blocking or forwarding state. VTP notifies STP when a trunk port becomes pruned or joined.

VTPv3

VTP Version 3 (VTPv3) was introduced in Cisco NX-OS release 7.2(0) and has the following features:

- Provides interoperability with switches configured with VTP version 1 or 2.
- Allows only the primary server to make VTP configuration changes.
- Supports 4K VLANs.
- Permits feature-specific primary servers. A switch can be a primary server for a specific feature database like MST or for the entire VLAN database.
- Provides enhanced security with hidden and secret passwords.
- Provides interoperability with private VLANs (PVLAN). PVLANs and VTPs are no longer mutually exclusive.
- Resolves the issue of VTP bombing. VTP bombing occurs when a server with a higher revision number and a wrong VTP database is inserted into the VTP domain. This may occur when a new switch is plugged into a stable VTP domain. The incorrect database is propagated to the domain and the earlier stable database is overwritten.

Restrictions for Configuring the VLAN Trunking Protocol

- You cannot manually configure VLANs on a device configured as a VTP client.
- PVLAN forward referencing is not supported with VTP.
- Administered VLANs are not displayed in the show output for all the VTP versions in the VTP client and server mode.

VTP Version 3 has the following software restrictions:

- On the Cisco Nexus 7000 Series switches, by default, the VTP version 3 is configured under the server mode. Whereas on the Cisco Nexus 9000 Series switches, by default, the VTP version 3 is configured under the transparent mode.

Default Settings

This table lists the default settings for VTP parameters.

Table 1: Default VTP Parameters

Parameters	Default
VTP	Disabled
VTP Mode	Transparent
VTP Domain	blank
VTP Version	1
VTP Pruning	Disabled
VTP per Interface	Enabled

Configuring VTP

You can configure VTP on Cisco NX-OS devices.

Note VLAN 1 is required on all trunk ports used for switch interconnects if VTP is used in transparent mode in the network. Disabling VLAN 1 from any of these ports prevents VTP from functioning properly in transparent mode.

Note Before Cisco NX-OS Release 5.1(1), VTP worked only in transparent mode. With Cisco NX-OS Release 7.2(0), VTP version 3 was introduced.

Before You Begin

Ensure that you are in the correct virtual device context (VDC) (or enter the **switchto vdc** command). VLAN names and IDs can be repeated in different VDCs, so you must confirm which VDC that you are working in.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **feature vtp**
3. switch(config)# **vtp domain** *domain-name*
4. switch(config)# **vtp version** {**1** | **2** | **3**}
5. switch(config)# **vtp mode** {**client** | **server** | **transparent** | **off**} [**vlan** | **mst** | **unknown**]
6. switch(config)# **vtp interface** *interface-name* [**only**]
7. switch(config)# **vtp file** *file-name*
8. switch(config)# **vtp password** *password-value* [**hidden** | **secret**]
9. switch(config)# **exit**
10. switch# **vtp primary** [*feature*] [**force**]
11. (Optional) switch# **show vtp status**
12. (Optional) switch# **show vtp counters**
13. (Optional) switch# **show vtp interface**
14. (Optional) switch# **show vtp password**
15. (Optional) switch# **show vtp devices [conflict]**
16. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **feature vtp**	Enables VTP on the device. The default is disabled.
Step 3	switch(config)# **vtp domain** *domain-name*	Specifies the name of the VTP domain that you want this device to join. The default is blank.
Step 4	switch(config)# **vtp version** {**1** | **2** | **3**}	Sets the VTP version that you want to use. The default is version 1. **Note** Version 3 is applicable for VTPv3 only and requires the configuration of VTP domain.
Step 5	switch(config)# **vtp mode** {**client** | **server** | **transparent** | **off**} [**vlan** | **mst** | **unknown**]	Sets the VTP mode to client, server, transparent, or off. The default server mode is for vlan instance and transparent is for mst instance.
Step 6	switch(config)# **vtp interface** *interface-name* [**only**]	Configures the interface name used by the VTP updater for this device.
Step 7	switch(config)# **vtp file** *file-name*	Specifies the ASCII filename of the IFS file system file where the VTP configuration is stored.
Step 8	switch(config)# **vtp password** *password-value* [**hidden** | **secret**] **Example:**	Specifies the password for the VTP administrative domain. Default value is taken from vlan.dat. The following options are applicable only on an image supporting VTP version 3:

	Command or Action	Purpose

	For Hidden:
	`Device(config)# ` **`vtp password helping hidden`**
	
	`Generating the secret associated to the`
	`password.`
	`Device# ` **`exit`**
	`Device# ` **`show vtp password`**
	`VTP Password:`
	`89914640C8D90868B6A0D8103847A733`
	
	Example:
	For Secret:
	`Device(config)# ` **`vtp password`**
	`89914640C8D90868B6A0D8103847A733 secret`
	`Device# ` **`exit`**
	`Device# ` **`show vtp password`**
	`VTP Password:`
	`89914640C8D90868B6A0D8103847A733`
		• Hidden–Password is not saved as clear text in vlan.data file. Instead, a hexadecimal secret key generated from the password is saved. This is displayed as the output of the **show vtp password**.
		• Secret–Use this keyword to directly configure the 32-character hexadecimalsecret key. System administrators can distribute this secret key instead of the clear text password.
		
		Note This command is applicable for VTP version 3 only.

Step 9	switch(config)# **exit**	Exits the configuration submode.

Step 10	switch# **vtp primary** [*feature*] [**force**]
	
	Example:
	`Device# ` **`vtp primary vlan`**
	
	`Enter VTP password:`
	`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`
		This command changes the operational state of a secondary server to primary and advertises the information to the entire VTP domain. If the password is configured as hidden, the user is prompted to re-enter the password after this command.
		
		Before the device takes over the role of primary, it attempts to discover servers that conflict this information and follows another primary server. If conflicting servers are discovered, the user must reconfirm the takeover of operational state and the subsequent overwriting of configuration.
		
		• feature–Configures the device as primary server for a specific feature database. For example, the MST database. Possible values are MST and VLAN. By default, the VLAN database is chosen.
		
		Note This command is applicable for VTPv3 only.

Step 11	switch# **show vtp status**	(Optional) Displays information about the VTP configuration on the device, such as the version, mode, and revision number.
Step 12	switch# **show vtp counters**	(Optional) Displays information about VTP advertisement statistics on the device.
Step 13	switch# **show vtp interface**	(Optional) Displays the list of VTP-enabled interfaces.
Step 14	switch# **show vtp password**	(Optional) Displays the password for the management VTP domain.

	Command or Action	Purpose

Step 15	switch# **show vtp devices [conflict]**
	Example:
	`Device# show vtp devices`
	`Gathering information from the domain,`
	`please wait.`
	`VTP Database Conf switch ID      Primary`
	`Server Revision   System Name`
	`             lict`
	`------------ ---- --------------`
	`-------------- ----------`
	`----------------------`
	`VLAN         Yes  00b0.8e50.d000`
	`000c.0412.6300 12354      main.cisco.com`
	`MST          No   00b0.8e50.d000`
	`0004.AB45.6000 24         main.cisco.com`
	`VLAN         Yes`
	`000c.0412.6300=000c.0412.6300 67`
	`qwerty.cisco.com`
		(Optional)
		This is a VTP version 3 command that displays information about neighbor switches. The information is not learned from the summary packet used for regular VTP packets. This command sends out a separate packet to collect information regarding neighbor switches running VTP version 3.

Step 16	switch# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

This example shows how to configure VTP in transparent mode for the device:

```
switch# configure terminal
switch(config)# feature vtp
switch(config)# vtp domain accounting
switch(config)# vtp version 2
switch(config)# vtp mode transparent
switch(config)# exit
switch#
```

Configuring VTP Pruning

You can configure VTP pruning on the Cisco NX-OS devices.

Before You Begin

You must enable VTP on the device.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **vtp pruning**
3. (Optional) switch(config)# **no vtp pruning**
4. (Optional) switch(config)# **show interface** *interface-identifier* **switchport**
5. switch(config)# **interface port-channel** *channel-number*
6. switch(config-if)# **switchport trunk pruning vlan** [**add** | **remove** | **except** | **none** | **all**] *VLAN-IDs*
7. switch(config-if)# **end**
8. (Optional) switch# **show vtp counters**
9. (Optional) switch# **clear vtp counters**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **vtp pruning**	Enables VTP pruning on the device. The default is disabled.
Step 3	switch(config)# **no vtp pruning**	(Optional) Disables VTP pruning on the device. The default is disabled.
Step 4	switch(config)# **show interface** *interface-identifier* **switchport**	(Optional) Displays the VTP pruning eligibility of the trunk port. The default is that all the VLANs from 2 to 1001 are pruning eligible.
Step 5	switch(config)# **interface port-channel** *channel-number*	Creates a port-channel interface and enter interface configuration mode.
Step 6	switch(config-if)# **switchport trunk pruning vlan** [**add** | **remove** | **except** | **none** | **all**] *VLAN-IDs*	Sets the specified VLANs to be VTP pruning eligible.
Step 7	switch(config-if)# **end**	returns to privileged EXEC mode.
Step 8	switch# **show vtp counters**	(Optional) Displays VTP pruning information and counters.
Step 9	switch# **clear vtp counters**	(Optional) Resets all the VTP pruning counter values.

This example shows how to set VLANs 9 to 54 to be pruning eligible and set VLANs 2 to 8 and 55 to 1001 as not eligible for VTP pruning:

```
switch(config-if)# switchport trunk pruning vlan 9-54
```

VLAN 1 is never pruning eligible, because it is a factory-default VLAN. VLANs 1002 to 1005 are reserved for Token Ring networks. The VLANs 1006 is not pruning eligible.