Configuring VTP V3

This chapter contains the following sections:

Configuring VTP V3

From Cisco NX-OS Release 7.2(0)N1(1), VLAN Trunk Protocol (VTP) V3 supports PVLAN integration, 4K VLAN integration, generic database transport mechanism, and VTP authentication mechanism.

VTP V3 Overview

VTP V3 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 V3 Modes

From Cisco NX-OS Release 7.2(0)N1(1), VTP V3 supports the following 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— Allows you to create, change, and delete VLANs on the local device. In VTP client mode, a switch stores the last known VTP information including the configuration revision number, on the bootflash. A VTP client might or might not start with a new configuration when it powers up.
- 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.

Note VTP client will move to transparent mode if there is any failure during updating VLAN database received from server. Following syslog message is displayed on console. `"VTP-2-VTP_MODE_TRANSPARENT_CREATE_SEQ_FAILED: VTP Mode changed to transparent since VTP vlan create/update failed"`. User need to change back the VTP mode to client to get latest database from server.

VTP V3 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 V3 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 the VTP V3 protocol. A VTP V3 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 V3 transparent mode, VTP relays all VTP packets, and pruning requires that the switch processes TLVs in the VTP V3 summary packets.

VTP V3 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 V3 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 V3 when a trunk port goes to the blocking or forwarding state. VTP V3 notifies STP when a trunk port becomes pruned or joined.

Configuring VTP V3

Note

- VLAN 1 is required on all trunk ports used for switch interconnects if VTP V3 is used in transparent mode in the network. Disabling VLAN 1 from any of these ports prevents VTP from functioning properly in transparent mode.
- The overlapping of system reserved VLANs between Cisco Nexus 6000 Series Switches and Cisco Nexus 5000 Series Switches causes interoperability issues. When a Cisco Catalyst 6000 Switch sends a VLAN reserved in the Cisco Nexus switch, it causes the Cisco Nexus 5000 and 6000 Series Switches to move to VTP Transparent Mode.

  Check the generated syslog messages in the Cisco Nexus Switches for information on the VLAN that caused the interoperability issue.

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.

Procedure

	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.
Step 5	Required: 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.

	Command or Action	Purpose
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:
	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`
		Specifies the password for the VTP administrative domain. Default value is taken from vlan.dat.
		The following options are applicable only on VTP V3:
		• 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.

	Command or Action	Purpose
		Note This command is applicable for VTPv3 only.
Step 11	(Optional) switch# **show vtp status**	Displays information about the VTP configuration on the device, such as the version, mode, and revision number.
Step 12	(Optional) switch# **show vtp counters**	Displays information about VTP advertisement statistics on the device.
Step 13	(Optional) switch# **show vtp interface**	Displays the list of VTP-enabled interfaces.
Step 14	(Optional) switch# **show vtp password**	Displays the password for the management VTP domain.

Step 15	(Optional) 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`
		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	(Optional) switch# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

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 V3 Pruning

Follow the steps given below to configure VTP V3 Pruning.

Procedure

	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	(Optional) switch(config)# **no vtp pruning**	Disables VTP pruning on the device. The default is disabled.
Step 4	(Optional) switch(config)# **show interface** *interface-identifier* **switchport**	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	Required: 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	(Optional) switch# **show vtp counters**	Displays VTP pruning information and counters.
Step 9	(Optional) switch# **clear vtp counters**	Resets all the VTP pruning counter values.