Cisco − Understanding and Configuring VLAN Trunk Protocol (

Table of Contents

Understanding and Configuring VLAN Trunk Protocol (VTP)....................1
- Interactive: This document offers customized analysis of your Cisco device.....1

Introduction....................1

Before You Begin....................2
- Conventions....................2
- Prerequisites....................2
- Components Used....................2

Understanding VTP....................2
- VTP Domain Name....................2
- VTP Mode....................4
- VTP Messages in Detail....................5

Other VTP Options....................8
- VTP V2....................8
- VTP Password....................8

VTP Pruning....................9

Using VTP in a Network....................9

VTP Configuration on Catalyst Switches....................9
- Catalyst 6000 Family Native IOS / Catalyst 4000 Cisco IOS (Supervisor III)....................9
- Catalyst 4000, 5000 or 6000 Family CatOS....................10
- Catalyst 2900XL, 3500XL, 2950, 3550....................10

Practical Examples....................10

VTP Troubleshooting and Caveats....................18
- How a Recently−Inserted Switch Can Cause Network Problems....................18
- Trunk Down Causing VTP Problems....................22
- VTP and Spanning Tree Protocol (Logical Spanning Tree Port)....................22
- The Case of VLAN 1....................24
- CatOS Switch Changes to VTP Transparent Mode, VTP−4−UNSUPPORTEDCFGRCVD:....................24
- Troubleshooting VTP Configuration Revision Number Errors Seen in the show vtp statistics Command....................28
- Troubleshooting VTP Configuration Digest Errors Seen in the show vtp statistics Command....................28

Conclusion....................29

Related Information....................29

Understanding and Configuring VLAN Trunk Protocol (VTP)

Interactive: This document offers customized analysis of your Cisco device.

Introduction
Before You Begin
Conventions
Prerequisites
Components Used
Understanding VTP
VTP Domain Name
VTP Mode
VTP Messages in Detail
Other VTP Options
VTP V2
VTP Password
VTP Pruning
Using VTP in a Network
VTP Configuration on Catalyst Switches
Catalyst 6000 Family Native IOS / Catalyst 4000 Cisco IOS (Supervisor III)
Catalyst 4000, 5000 or 6000 Family CatOS
Catalyst 2900XL, 3500XL, 2950, 3550
Practical Examples
VTP Troubleshooting and Caveats
How a Recently−Inserted Switch Can Cause Network Problems
Trunk Down Causing VTP Problems
VTP and Spanning Tree Protocol (Logical Spanning Tree Port)
The Case of VLAN 1
CatOS Switch Changes to VTP Transparent Mode, VTP−4−UNSUPPORTEDCFGRCVD:
Troubleshooting VTP Configuration Revision Number Errors Seen in the show vtp statistics Command
Troubleshooting VTP Configuration Digest Errors Seen in the show vtp statistics Command
Conclusion
Related Information

Introduction

Virtual Local Area Network (VLAN) Trunk Protocol (VTP) reduces administration in a switched network. When you configure a new VLAN on one VTP server, the VLAN is distributed through all switches in the domain. This reduces the need of configuring the same VLAN everywhere. VTP is a Cisco−proprietary protocol that is available on most of the Cisco Catalyst Family products.

Before You Begin

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Prerequisites

There are no specific prerequisites for this document.

Components Used

This document is not restricted to specific software and hardware versions.

Understanding VTP

VTP−capable devices can be configured to operate in the following three modes:

- The **VTP Server** maintains a full list of all VLANs within the VTP domain. Information is stored in nonvolatile random−access memory (NVRAM). The server can add, delete, and rename VLANs.
- The **VTP Client** also maintains a full list of all VLANs. However, it will not store in NVRAM. The client can not add, delete, or rename VLANs. Any changes made must be received from a VTP server advertisement.
- The **VTP Transparent** does not participate in VTP. However, it will pass on a VTP advertisement. VLAN, as defined, is only local to the switch and is stored in NVRAM.

VTP operates through VTP messages (multicast messages) sent to a particular MAC address (01−00−0C−CC−CC−CC). Note that VTP advertisements only travel through trunk ports. Therefore, VTP information only flows through the Inter−Switch Link (ISL), 802.1q port, or LAN emulation (LANE), when the trunk is up, after Dynamic Inter−Switch Link (DISL) or DTP convergence.

VTP messages are only carried through VLAN 1. To send VTP messages through a LANE cloud, be sure that the LANE client (for the LANE mapped to VLAN 1) is up on the LANE port.

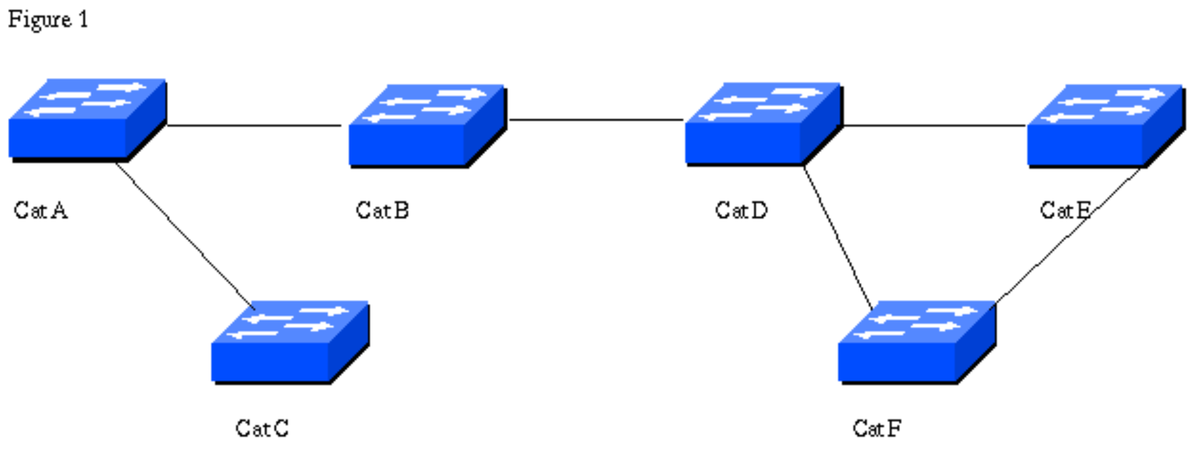
VTP Domain Name

In order to use VTP, you must assign a VTP domain name to each switch. VTP information will remain only within the same VLAN domain. The following are conditions for a VTP domain:

- Each Catalyst switch in a domain should be assigned the same VTP domain name.
- The Catalyst switches must be adjacent.
-

Trunking must be enabled between all Catalyst switches.

If any one of the previous conditions is not met, the VTP domain is broken and information will not travel between the two separate parts.



To further explain this first concept, refer to Figure 1 and consider the following scenarios (assuming all devices are on a VTP server):

- If Catalysts A, B, and C are in VTP domain EUROPE and Catalysts D, E, and F are in VTP domain ASIA (assuming all links are trunk), the VLAN information will not flow between the two domains. If you create VLAN 2 and 3 in Catalysts B, then Catalyst D, E, and F will never learn about VLAN 2 and 3, unless you configure them specifically on one of the switches in the VTP domain ASIA.
- In exactly the same way, if Catalysts A, B, and C are in domain EUROPE and if Catalysts D, E, and F are in domain ASIA (assuming all links are trunk), then you will have VLAN 4 existing in both domains. If you clear VLAN 4 in Catalyst D, VLAN 4 will also be cleared in Catalysts E and F. However, VLAN 4 will not be cleared (will still exist) in Catalysts A, B, and C.
- Assume that all six Catalysts are in VTP domain EUROPE. If you then create VLAN 5 on Catalysts B, it will be propagated to all of the other Catalysts. However, if the link between Catalysts B and Catalyst D stops, the trunking to VLAN 1 falls down. If we then create VLAN 6 on Catalysts B, it will not be propagated to Catalysts D, E, and F until the trunk is back up.
- Assume that the link between Catalysts A and Catalysts C is no longer a trunk. Assign the link to VLAN 1. Then, despite the fact that all Catalysts are in the same VTP domain, the domain is broken in two pieces (Catalysts C in one and Catalysts A, B, D, E, and F in the other). The VTP information does not flow between them.
- In this last scenario, Catalysts A is in VTP domain ASIA and Catalysts B, C, D, E, and F are in VTP domain EUROPE (all links are trunk). If we create a VLAN in Catalysts B, then Catalysts D, E, and F will receive it. However, Catalysts A will not receive this VLAN because it is in a different VTP domain. Additionally, Catalysts C will not be propagated by this VLAN. In fact, domain EUROPE is discontinued. Since Catalysts B and Catalysts C are not adjacent in the same domain, domain

EUROPE is not the same for Catalysts C as it is for Catalysts B, D, E, and F.

Listed below are the two methods for being included in a VTP domain:

- Manually configure the VTP domain name (on the VTP server and the VTP client).
- If a switch has no VTP domain name configured, it will receive the VTP domain name from an attached switch through the trunk port (if one is available). The switch configuration defaults to a VTP server, without a VTP domain name. When a new set of Catalysts are connected by a trunk, you only need to configure the VTP domain name on one switch. The other switches will be notified of the VTP domain name through the first summary advertisement.

Notes:

- If a switch is configured as a VTP server without a VTP domain name, you cannot configure a VLAN on it.
- If a new Catalyst is attached in the border of two VTP domains, the new Catalyst will keep the domain name of the first switch that sends it a summary advertisement. The only way to attach this switch to another VTP domain is to manually set a different VTP domain name.
- DISL sends the VTP domain name in a DISL packet. Therefore, if you have two ends of a link belonging to a different VTP domain, the trunk will not come up if you use DISL. In this special case, you need to configure the trunk mode as "on", on both sides, to prevent DISL from running.

VTP Mode

As explained earlier, VTP can run in three modes: server, client, and transparent. Below is a detailed explanation of the differences between these modes.

Feature	Server	Client	Transparent
Source VTP messages	Yes	Yes	No
Listen to VTP messages	Yes	Yes	No
Create VLANs	Yes	No	Yes (locally significant only)
Remember VLANs	Yes	No	Yes (locally significant only)

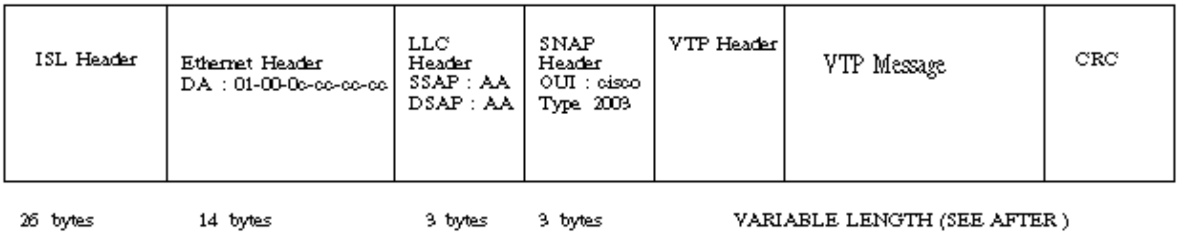
In the table above, "Source VTP message" refers to the sending of VTP messages to all trunks. "Listen to VTP messages" refers to listening to the Media Access Control (MAC) address 01−00−0C−CC−CC−CC and processing the VTP update.

There is no difference in the way that the server and the client source listen to VTP messages. The only differences between the server and the client is that VLAN cannot be configured directly on a client, and the client does not remember the VLAN after a reboot (no VLAN information is written in NVRAM).

Transparent mode indicates that a switch does not participate in VTP. Therefore, the switch ignores all received VTP messages. The switch will, however, send messages on to all other outgoing trunks.

VTP Messages in Detail

VTP packets are sent in either ISL frames or in dot1q frames. These packets are sent to the destination MAC address 01−00−0c−cc−cc−cc with a Logical Link Control (LLC) code of Subnetwork Access Protocol (SNAP) (AAAA) and a type of 2003 (in the snap header). Below is the format of a VTP packet encapsulated in ISL frames:



You can, of course, have a VTP packet inside 802.1Q frames. In that case, the ISL header and cyclic redundancy check (CRC) would be replaced by dot1q tagging.

Now let's look into the detail of a VTP packet. The format of the VTP header can vary depending on the type of VTP message. However, they all contain the following fields in the header:

- VTP protocol version : 1 or 2
- VTP message types:
  - Summary advertisements
  - Subset advertisement
  - Advertisement requests
  - VTP join messages
- Management domain length
- Management domain name

Configuration Revision Number

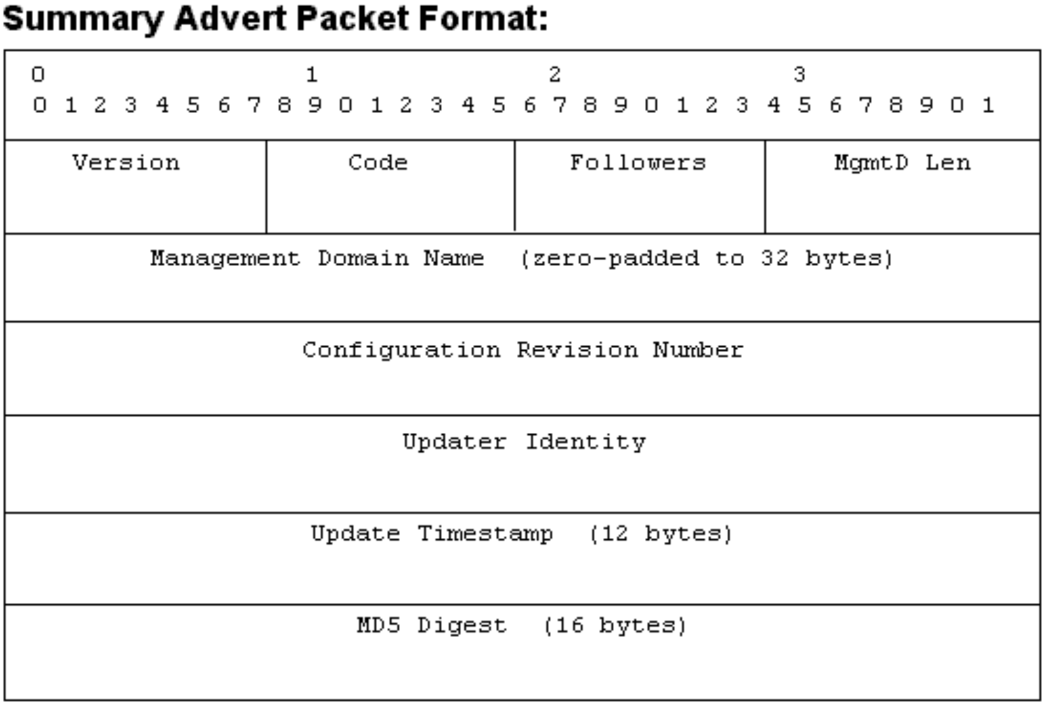
The configuration revision number is a 32 bit number that indicates the level of revision for a VTP packet. Each VTP device tracks it's own VTP configuration revision number, and most of the VTP packets contain the VTP configuration revision number of the sender.

This information is used to determine whether the received information is more recent than the current version. Each time you make a VLAN change in a VTP device, the configuration revision is incremented, one by one. In order to reset the configuration revision of a switch, simply change the VTP domain name and then change it back to the original name.

Summary Advertisements

By default, Catalysts issue summary advertisements in five minute increments. Summary advertisements inform adjacent Catalysts of the current VTP domain name and the configuration revision number.

When the switch receives a summary advertisement packet, it compares the VTP domain name. If the name is different, the switch simply ignores the packet. If the name is the same, the switch then compares the configuration revision. If its own configuration revision is higher or equal, the packet is ignored. If it is lower, an advertisement request is sent.



Summary Advert Packet Format:

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
```

Version	Code	Followers	MgmtD Len
Management Domain Name (zero-padded to 32 bytes)			
Configuration Revision Number			
Updater Identity			
Update Timestamp (12 bytes)			
MD5 Digest (16 bytes)			

The following list clarifies the meaning of these fields in the summary advert packet:

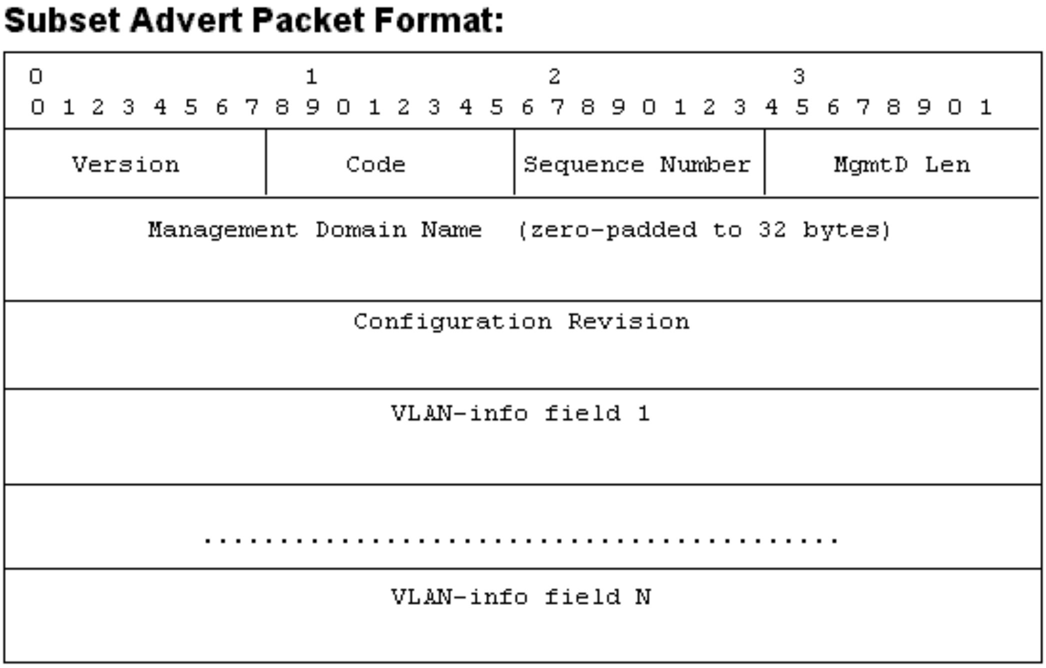
- Followers indicate that this packet is followed by a Subset Advertisement packet.
- The updater identity is the IP address of the last switch which has incremented the configuration revision.
-

Update timestamps are the date and time of the last increment of the configuration revision.

- Message Digest 5 (MD5) carries the VTP password if it is configured and used to authenticate the validation of a VTP update.

Subset Advertisements

When you add, delete, or change a VLAN in a Catalyst, the server Catalyst, where the changes were made, increments the configuration revision and issues a summary advertisement, followed by one or several subset advertisements. A subset advertisement contains a list of VLAN information. If there are several VLANS, more than one subset advertisement may be required in order to advertise them all.

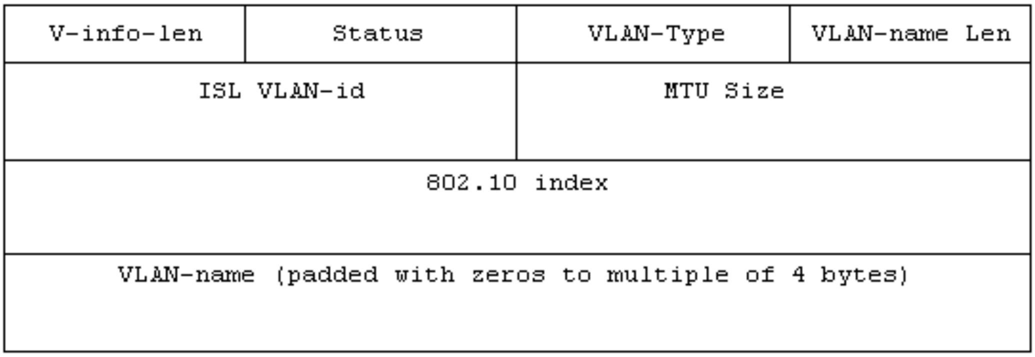


Subset Advert Packet Format:

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
```

Version	Code	Sequence Number	MgmtD Len
Management Domain Name (zero-padded to 32 bytes)			
Configuration Revision			
VLAN-info field 1			
....			
VLAN-info field N			

The following formatted example shows that each VLAN information field contains information for a different VLAN (ordered with lowered−valued ISL VLAN IDs occurring first):



V-info-len	Status	VLAN-Type	VLAN-name Len
ISL VLAN-id		MTU Size	
802.10 index			
VLAN-name (padded with zeros to multiple of 4 bytes)			

Most of the fields in this packet are easy to understand. Below are two clarifications:

- Code: 0x02 for Subset Advertisement

-

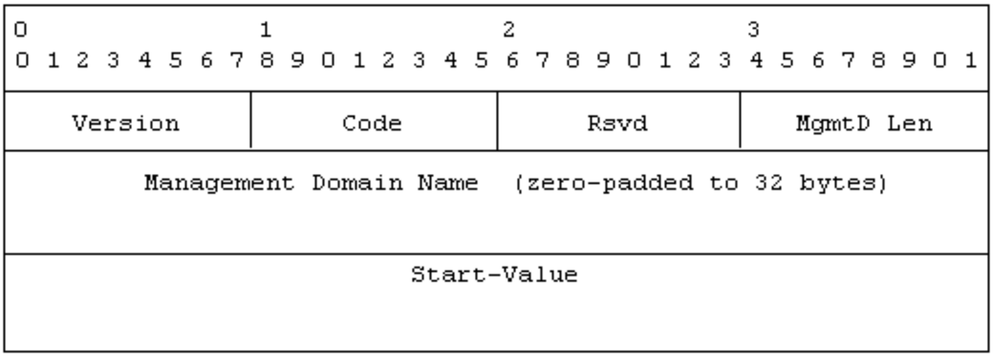
Sequence number: sequence of the packet in the stream of packets following a summary advertisement. The sequence starts with 1.

Advertisement Requests

A switch needs a VTP advertisement request in the following situations:

- The switch has been reset.
- The VTP domain name has been changed.
- The switch has received a VTP summary advertisement with a higher configuration revision than its own.

Upon receipt of an advertisement request, a VTP device sends a summary advertisement, followed by one or more subset advertisements. Below is an example:



0 1 2 3 4 5 6 7	1 8 9 0 1 2 3 4 5	2 6 7 8 9 0 1 2 3	3 4 5 6 7 8 9 0 1
Version	Code	Rsvd	MgmtD Len
Management Domain Name (zero-padded to 32 bytes)			
Start-Value			

- Code: 0x03 for advertisement request
- Start Value: Used in cases where there are several subset advertisements. If the first (N) subset advertisement has been received and the subsequent one (N+1) has not, only request advertisements from the (N+1)

Other VTP Options

VTP V2

VTP Version 2 (V2) is not much different than VTP Version 1 (V1). The major difference is that VTP V2 introduces the support for Token Ring VLANs. If you are using Token Ring VLANs, you need to enable VTP V2. Otherwise, there is no reason to use VTP V2.

VTP Password

If you configure a password for VTP, it needs to be configured on all switches in the VTP domain and it needs to be the same password. The VTP password you configure is translated using an algorithm in a 16 bytes word

(MD5 value) carried in all summary−advertisement VTP packet.

VTP Pruning

VTP ensures that all switches in the VTP domain are aware of all VLANs. There are occasions, however, when VTP can create unnecessary traffic. All unknown unicasts and broadcasts in a VLAN are flooded all over the VLAN. All switches in the network receive all broadcasts, even in situations where few users are connected in that VLAN. VTP pruning is a feature used to eliminate (prune) this unnecessary traffic.

Using VTP in a Network

By default, all switches are configured to be VTP servers. This is suitable for small scale networks where the size of the VLAN information will be small and easily stored in all switches (in NVRAM). In a large network, a judgment call must be made at some point when the NVRAM storage needed is wasted when duplicated on every switch. At this point, the network administrator should pick a few well endowed switches and keep them as VTP servers. Everything else participating in VTP can be turned into a client. The number of VTP servers should be picked with the amount of redundancy desired in the network.

VTP Configuration on Catalyst Switches

This section provides some basic commands to configure VTP on the most commonly used Catalyst switches.

Note: The Catalyst 2948G−L3 and Catalyst 4908G−L3 Layer 3 switches do not support several Layer 2−oriented protocols, such as VTP, DTP, and PAgP, found on other Catalyst switches.

Catalyst 6000 Family Native IOS / Catalyst 4000 Cisco IOS (Supervisor III)

In Cisco IOS, the VTP domain name, VTP mode and VLANs can be configured in VLAN configuration mode. In the exec mode, issue the following commands to enter in VLAN configuration mode:

```
Router#vlan database

!−−− This command is entered in Privileged EXEC mode, not in global configuration mode.


Router(vlan)#

!−−− This is VLAN configuration mode.
```

To set the VTP domain name, enter:

```
Router(vlan)#vtp mode {client | server | transparent}
```

To exit from VLAN configuration mode use, use exit command, end or ^z command doesn't work here.

```
Router(vlan)#end

% Invalid input detected at '^' marker.
Router(vlan)#^Z
Router(vlan)#
Router(vlan)#exit
```

```
APPLY completed.
Exiting....
Router#
```

To monitor the VTP operation and status, enter:

```
Router# show vtp status

Router# show vtp counters
```

Catalyst 4000, 5000 or 6000 Family CatOS

Issue the following commands:

To set the domain name, enter:

```
set vtp domain 'name'
```

To set the mode, enter:

```
set vtp mode [server|client|transparent]
```

To monitor the VTP operation and status, enter:

```
show vtp domain
show vtp stat
```

Catalyst 2900XL, 3500XL, 2950, 3550

From the VLAN database mode, issue the following commands:

```
vtp [client | server | transparent]
vtp domain 'name'
```

From the Enable mode, use the following commands to monitor VTP operation:

```
show vtp counters
show vtp status
```

Note: The Catalyst 2900XL series switches with Cisco IOS release 11.2(8)SA4 and later support VTP protocol. The Cisco IOS Release 11.2(8)SA3 and older code do not support VTP protocol on Catalyst 2900XL series switches.

Practical Examples

This first example involves two Catalyst 4000s that are connected together by a FastEthernet link:

1. "Bing" is a new switch that has no VTP domain name and no VLAN. "Clic" is an existing, running switch with 12 VLANs in VTP domain test.

2.

Note on the output of the **show vtp domain** command below that VTP version is set at two, which means the switch is VTP V2 capable, but it does not run VTP V2 in this case. It will only run VTP V2 if the V2 mode is enabled by using the **set vtp v2 enable** command:

```
bing (enable) show vtp dom
Domain Name                      Domain Index VTP Version Local Mode  Password
-------------------------------- ------------ ----------- ----------- ----------
                                   1            2           server      -

Vlan-count Max-vlan-storage Config Revision Notifications
---------- ---------------- --------------- -------------
5          1023             0               disabled

Last Updater    V2 Mode  Pruning  PruneEligible on Vlans
--------------- -------- -------- -------------------------
0.0.0.0         disabled disabled 2-1000
bing (enable)
bing (enable)
bing (enable) show vlan
VLAN Name                             Status    IfIndex Mod/Ports, Vlans
---- -------------------------------- --------- ------- ------------------------
1    default                          active    67      2/1-2,2/4-48
                                                      3/1-6
1002 fddi-default                     active    68
1003 token-ring-default               active    71
1004 fddinet-default                  active    69
1005 trnet-default                    active    70


clic (enable)  show vtp dom
Domain Name                      Domain Index VTP Version Local Mode  Password
-------------------------------- ------------ ----------- ----------- ----------
test                             1            2           server      -

Vlan-count Max-vlan-storage Config Revision Notifications
---------- ---------------- --------------- -------------
12         1023             11              disabled

Last Updater    V2 Mode  Pruning  PruneEligible on Vlans
--------------- -------- -------- -------------------------
0.0.0.0         disabled disabled 2-1000
clic (enable) show vlan
VLAN Name                             Status    IfIndex Mod/Ports, Vlans
---- -------------------------------- --------- ------- ------------------------
1    default                          active    65      2/1-2,2/4-50
2    VLAN0002                         active    77
3    VLAN0003                         active    78      2/3
4    VLAN0004                         active    79
5    VLAN0005                         active    73
6    VLAN0006                         active    74
7    VLAN0007                         active    76
10   VLAN0010                         active    80
1002 fddi-default                     active    66
1003 token-ring-default               active    69
1004 fddinet-default                  active    67
1005 trnet-default                    active    68      68
```

3.

Below, a trunk is created between the two switches. Notice how they synchronize and watch the VTP packet exchange:

```
MAC 005014BB63FD is clic

MAC 003019798CFD is bing
```

4. Clic sends a summary advertisement to Bing. Bing learns the VTP domain name from this packet (Frame 1, below):

```
On bing :
received vtp packet: mNo = 2 pNo = 1
VTP: i summary, domain = test, rev = 11, followers = 0

!--- Received first summary advertisement.

domain change notification sent
VTP: transitioning from null to test domain

!--- Get VTP domain name.

VTP: summary packet rev 11 greater than domain test rev 0
VTP: domain test currently not in updating state
VTP: summary packet with followers field zero

------------------FRAME 1-----------------------------------
DLC:  ----- DLC Header -----
      DLC:
      DLC:  Frame 1988 arrived at  15:01:00.1223; frame size is 99 (0063 hex) bytes.
      DLC:  Destination = Multicast 01000CCCCCCC
      DLC:  Source      = Station 005014BB63FD
      DLC:  802.3 length = 85
      DLC:
LLC:  ----- LLC Header -----
      LLC:
      LLC:  DSAP Address = AA, DSAP IG Bit = 00 (Individual Address)
      LLC:  SSAP Address = AA, SSAP CR Bit = 00 (Command)
      LLC:  Unnumbered frame: UI
      LLC:
SNAP: ----- SNAP Header -----
      SNAP:
      SNAP: Vendor ID = Cisco1
      SNAP: Type = 2003 (VTP)
      SNAP:
VTP: ----- Cisco Virtual Trunk Protocol (VTP) Packet -----
      VTP:
      VTP: Version                          = 1
      VTP: Message type                     = 0x01 (Summary-Advert)
      VTP: Number of Subset-Advert messages = 0
      VTP: Length of management domain name = 4
      VTP: Management domain name           = "test"
      VTP: Number of Padding bytes          = 28
      VTP: Configuration revision number    = 0x0000000b
      VTP: Updater Identity IP address      = 0.0.0.0
      VTP: Update Timestamp                 = "930525053753"
      VTP: MD5 Digest value                 = 0x857610862F3015F0
      VTP:                                    0x220A52427247A7A0
-----------------------------------------------------------
```

5. With trace set, Bing receives a summary advertisement with no followers. Therefore, Bing updates its domain name and sends advertisement requests to obtain the VLAN information (Frame 2, below):

```
On bing :

VTP: tx vtp request, domain test, start value 0

!-- Advert request is sent.


----------------------FRAME 2--------------------------------
DLC:  ----- DLC Header -----
      DLC:
      DLC:  Frame 1683 arrived at  17:38:55.9383; frame size is 60 (003C hex) bytes.
      DLC:  Destination = Multicast 01000CCCCCCC
      DLC:  Source      = Station 003019798CFD
      DLC:  802.3 length = 46
      DLC:
LLC:  ----- LLC Header -----
      LLC:
      LLC:  DSAP Address = AA, DSAP IG Bit = 00 (Individual Address)
      LLC:  SSAP Address = AA, SSAP CR Bit = 00 (Command)
      LLC:  Unnumbered frame: UI
      LLC:
SNAP: ----- SNAP Header -----
      SNAP:
      SNAP: Vendor ID = Cisco1
      SNAP: Type = 2003 (VTP)
      SNAP:
VTP: ----- Cisco Virtual Trunk Protocol (VTP) Packet -----
      VTP:
      VTP: Version                          = 1
      VTP: Message type                     = 0x03 (Advert-Request)
      VTP: Reserved
      VTP: Length of management domain name = 4
      VTP: Management domain name           = "test"
      VTP: Padding bytes                    = 28
      VTP: Start value                      = 0 (all VLANs)
--------------------------------------------------------
```

6. Clic sends another summary advertisement (with field followers) to VLAN 1. This packet is followed by the subset advertisement (Frame 3, below) that contains all VLANs. Then, Bing configures all of the VLANs:

```
on Bing :
received vtp packet: mNo = 2 pNo = 1
VTP: i summary, domain = test, rev = 11, followers = 1

!--- Received second summary advert.

VTP: domain test, current rev = 0 found for summary pkt
VTP: summary packet rev 11 greater than domain test rev 0

!--- The configuration revision is higher than ours.

VTP: domain test currently not in updating state
received vtp packet: mNo = 2 pNo = 1
VTP: i subset, domain = test, rev = 11, seq = 1, length = 344

!--- Received subset advert.

VTP: domain test, current rev = 0 found for subset pkt
domain change notification sent
vlan 1 unknown tlv change notification sent
vlan 2 unknown tlv change notification sent
vtp_vlan_change_notification: vlan = 2, mode = 1
(ADD,ACTIVE), mNo = 2 pNo = 1 vlan = 2
vlan 3 unknown tlv change notification sent
vtp_vlan_change_notification: vlan = 3, mode = 1
(ADD,ACTIVE), mNo = 2 pNo = 1 vlan = 3
vlan 4 unknown tlv change notification sent
vtp_vlan_change_notification: vlan = 4, mode = 1
(ADD,ACTIVE), mNo = 2 pNo = 1 vlan = 4
vlan 5 unknown tlv change notification sent
vtp_vlan_change_notification: vlan = 5, mode = 1
(ADD,ACTIVE), mNo = 2 pNo = 1 vlan = 5
vlan 6 unknown tlv change notification sent
vtp_vlan_change_notification: vlan = 6, mode = 1
(ADD,ACTIVE), mNo = 2 pNo = 1 vlan = 6
vlan 7 unknown tlv change notification sent
vtp_vlan_change_notification: vlan = 7, mode = 1
(ADD,ACTIVE), mNo = 2 pNo = 1 vlan = 7

-----------------FRAME 3----------------------------------
DLC:  ----- DLC Header -----
      DLC:
      DLC:  Frame 2008 arrived at  15:01:03.9661; frame size is 99 (0063 hex) bytes.
      DLC:  Destination = Multicast 01000CCCCCCC
      DLC:  Source      = Station 003019798CFD
      DLC:  802.3 length = 85
      DLC:
LLC:  ----- LLC Header -----
      LLC:
      LLC:  DSAP Address = AA, DSAP IG Bit = 00 (Individual Address)
      LLC:  SSAP Address = AA, SSAP CR Bit = 00 (Command)
      LLC:  Unnumbered frame: UI
      LLC:
SNAP: ----- SNAP Header -----
      SNAP:
      SNAP: Vendor ID = Cisco1
      SNAP: Type = 2003 (VTP)
      SNAP:
VTP: ----- Cisco Virtual Trunk Protocol (VTP) Packet -----
      VTP:
      VTP: Version                          = 1
      VTP: Message type                     = 0x01 (Summary-Advert)
      VTP: Number of Subset-Advert messages = 1

          !--- Here the numbers as followers.

      VTP: Length of management domain name = 4
      VTP: Management domain name           = "test"
      VTP: Number of Padding bytes          = 28
      VTP: Configuration revision number    = 0x0000000b
      VTP: Updater Identity IP address      = 0.0.0.0
      VTP: Update Timestamp                 = "930525053753"
      VTP: MD5 Digest value                 = 0x857610862F3015F0
      VTP:                                    0x220A52427247A7A0


DLC:  ----- DLC Header -----
      DLC:
      DLC:  Frame 2009 arrived at  15:01:03.9664; frame size is 366 (016E hex) bytes
      DLC:  Destination = Multicast 01000CCCCCCC
      DLC:  Source      = Station 003019798CFD
      DLC:  802.3 length = 352
      DLC:
LLC:  ----- LLC Header -----
```

```
      LLC:
      LLC:  DSAP Address = AA, DSAP IG Bit = 00 (Individual Address)
      LLC:  SSAP Address = AA, SSAP CR Bit = 00 (Command)
      LLC:  Unnumbered frame: UI
      LLC:
SNAP: −−−−− SNAP Header −−−−−
      SNAP:
      SNAP: Vendor ID = Cisco1
      SNAP: Type = 2003 (VTP)
      SNAP:
VTP: −−−−− Cisco Virtual Trunk Protocol (VTP) Packet −−−−−
      VTP:
      VTP: Version                          = 1
      VTP: Message type                     = 0x02 (Subset−Advert)
      VTP: Sequence number                  = 1
      VTP: Management Domain Name length    = 4
      VTP: Management Domain Name           = "test"
      VTP: Number of Padding bytes          = 28
      VTP: Configuration revision number    = 0x0000000b
      VTP:
      VTP: VLAN Information Field # 1:
      VTP: VLAN information field length    = 20
      VTP: VLAN Status                      = 00 (Operational)
      VTP: VLAN type                        = 1 (Ethernet)
      VTP: Length of VLAN name              = 7
      VTP: ISL VLAN−id                      = 1
      VTP: MTU size                         = 1500
      VTP: 802.10 SAID field                = 100001
      VTP: VLAN Name                        = "default"
      VTP: # padding bytes in VLAN Name     = 1
      VTP:
      VTP: VLAN Information Field # 2:
      VTP: VLAN information field length    = 20
      VTP: VLAN Status                      = 00 (Operational)
      VTP: VLAN type                        = 1 (Ethernet)
      VTP: Length of VLAN name              = 8
      VTP: ISL VLAN−id                      = 2
      VTP: MTU size                         = 1500
      VTP: 802.10 SAID field                = 100002
      VTP: VLAN Name                        = "VLAN0002"
      VTP: # padding bytes in VLAN Name     = 0
      VTP:
      VTP: VLAN Information Field # 3:
      VTP: VLAN information field length    = 20
      VTP: VLAN Status                      = 00 (Operational)
      VTP: VLAN type                        = 1 (Ethernet)
      VTP: Length of VLAN name              = 8
      VTP: ISL VLAN−id                      = 3
      VTP: MTU size                         = 1500
      VTP: 802.10 SAID field                = 100003
      VTP: VLAN Name                        = "VLAN0003"
      VTP: # padding bytes in VLAN Name     = 0
      VTP:
      VTP: VLAN Information Field # 4:
      VTP: VLAN information field length    = 20
      VTP: VLAN Status                      = 00 (Operational)
      VTP: VLAN type                        = 1 (Ethernet)
      VTP: Length of VLAN name              = 8
      VTP: ISL VLAN−id                      = 4
      VTP: MTU size                         = 1500
      VTP: 802.10 SAID field                = 100004
      VTP: VLAN Name                        = "VLAN0004"
      VTP: # padding bytes in VLAN Name     = 0
      VTP:
```

```
VTP: VLAN Information Field # 5:
VTP: VLAN information field length    = 20
VTP: VLAN Status                      = 00 (Operational)
VTP: VLAN type                        = 1 (Ethernet)
VTP: Length of VLAN name              = 8
VTP: ISL VLAN−id                      = 5
VTP: MTU size                         = 1500
VTP: 802.10 SAID field                = 100005
VTP: VLAN Name                        = "VLAN0005"
VTP: # padding bytes in VLAN Name     = 0
VTP:
VTP: VLAN Information Field # 6:
VTP: VLAN information field length    = 20
VTP: VLAN Status                      = 00 (Operational)
VTP: VLAN type                        = 1 (Ethernet)
VTP: Length of VLAN name              = 8
VTP: ISL VLAN−id                      = 6
VTP: MTU size                         = 1500
VTP: 802.10 SAID field                = 100006
VTP: VLAN Name                        = "VLAN0006"
VTP: # padding bytes in VLAN Name     = 0
VTP:
VTP: VLAN Information Field # 7:
VTP: VLAN information field length    = 20
VTP: VLAN Status                      = 00 (Operational)
VTP: VLAN type                        = 1 (Ethernet)
VTP: Length of VLAN name              = 8
VTP: ISL VLAN−id                      = 7
VTP: MTU size                         = 1500
VTP: 802.10 SAID field                = 100007
VTP: VLAN Name                        = "VLAN0007"
VTP: # padding bytes in VLAN Name     = 0
VTP:
VTP: VLAN Information Field # 8:
VTP: VLAN information field length    = 20
VTP: VLAN Status                      = 00 (Operational)
VTP: VLAN type                        = 1 (Ethernet)
VTP: Length of VLAN name              = 8
VTP: ISL VLAN−id                      = 10
VTP: MTU size                         = 1500
VTP: 802.10 SAID field                = 100010
VTP: VLAN Name                        = "VLAN0010"
VTP: # padding bytes in VLAN Name     = 0
VTP:
VTP: VLAN Information Field # 9:
VTP: VLAN information field length    = 32
VTP: VLAN Status                      = 00 (Operational)
VTP: VLAN type                        = 2 (FDDI)
VTP: Length of VLAN name              = 12
VTP: ISL VLAN−id                      = 1002
VTP: MTU size                         = 1500
VTP: 802.10 SAID field                = 101002
VTP: VLAN Name                        = "fddi−default"
VTP: # padding bytes in VLAN Name     = 0
VTP: Reserved 8 bytes
VTP:
VTP: VLAN Information Field # 10:
VTP: VLAN information field length    = 40
VTP: VLAN Status                      = 00 (Operational)
VTP: VLAN type                        = 3 (Token−Ring)
VTP: Length of VLAN name              = 18
VTP: ISL VLAN−id                      = 1003
VTP: MTU size                         = 1500
VTP: 802.10 SAID field                = 101003
```

```
      VTP: VLAN Name                        = "token-ring-default"
      VTP: # padding bytes in VLAN Name     = 2
      VTP: Reserved 8 bytes
      VTP:
      VTP: VLAN Information Field # 11:
      VTP: VLAN information field length    = 36
      VTP: VLAN Status                      = 00 (Operational)
      VTP: VLAN type                        = 4 (FDDI-Net)
      VTP: Length of VLAN name              = 15
      VTP: ISL VLAN-id                      = 1004
      VTP: MTU size                         = 1500
      VTP: 802.10 SAID field                = 101004
      VTP: VLAN Name                        = "fddinet-default"
      VTP: # padding bytes in VLAN Name     = 1
      VTP: Reserved 8 bytes
      VTP:
      VTP: VLAN Information Field # 12:
      VTP: VLAN information field length    = 36
      VTP: VLAN Status                      = 00 (Operational)
      VTP: VLAN type                        = 5 (TR-Net)
      VTP: Length of VLAN name              = 13
      VTP: ISL VLAN-id                      = 1005
      VTP: MTU size                         = 1500
      VTP: 802.10 SAID field                = 101005
      VTP: VLAN Name                        = "trnet-default"
      VTP: # padding bytes in VLAN Name     = 3
      VTP: Reserved 8 bytes
----------------------------------------------------------------
```

7. At this point, both switches are synchronized:

```
bing (enable) show vtp dom
Domain Name                       Domain Index VTP Version Local Mode  Password
-------------------------------- ------------ ----------- ----------- ----------
test                              1            2           server      -

Vlan-count Max-vlan-storage Config Revision Notifications
---------- ---------------- --------------- -------------
12         1023             11              disabled

Last Updater    V2 Mode  Pruning  PruneEligible on Vlans
--------------- -------- -------- -------------------------
0.0.0.0         disabled disabled 2-1000
bing (enable) show vlan
VLAN Name                             Status    IfIndex Mod/Ports, Vlans
---- -------------------------------- --------- ------- ------------------------
1    default                          active    127     2/2-48
                                                        3/1-6
2    VLAN0002                         active    132
3    VLAN0003                         active    133
4    VLAN0004                         active    134
5    VLAN0005                         active    135
6    VLAN0006                         active    136
7    VLAN0007                         active    137
10   VLAN0010                         active    138
1002 fddi-default                     active    128
1003 token-ring-default               active    131
1004 fddinet-default                  active    129
1005 trnet-default                    active    130
```

The following example shows how to verify the VTP configuration using Catalyst 6000 Native IOS.

```
Router# show vtp status


VTP Version: 2
Configuration Revision:           247
Maximum VLANs supported locally: 1005
Number of existing VLANs:          33
VTP Operating Mode:            Client
VTP Domain Name:          Lab_Network
VTP Pruning Mode:             Enabled
VTP V2 Mode:                 Disabled
VTP Traps Generation:        Disabled
MD5 digest: 0x45 0x52 0xB6 0xFD 0x63 0xC8 0x49 0x80
Configuration last modified by 0.0.0.0 at 8−12−99 15:04:49
Router#
```

The following example shows how to display VTP statistics in Catalyst 6000 Native IOS.

```
Router# show vtp counters
VTP statistics:
Summary advertisements received: 7
Subset advertisements received: 5
Request advertisements received: 0
Summary advertisements transmitted: 997
Subset advertisements transmitted: 13
Request advertisements transmitted: 3
Number of config revision errors: 0
Number of config digest errors: 0
Number of V1 summary errors: 0
VTP pruning statistics:

Trunk            Join Transmitted Join Received    Summary advts received
                                                   from on−pruning−capable device
---------------- ---------------- ---------------- ---------------------------
Fa5/8             43071            42766            5
```

VTP Troubleshooting and Caveats

Below are some common troubleshooting situations for VTP.

How a Recently−Inserted Switch Can Cause Network Problems

This problem occurs when you have a large switched domain, which is all in the same VTP domain, and you want to add one switch in the network.

This switch was previously used in the lab and a good VTP domain name was entered. It was configured as a VTP client, and connected to the rest of the network. Then, the ISL link was brought up to the rest of the network. In just a few seconds, the whole network is down. What could have happened?

The configuration revision of the switch you inserted was higher than the configuration revision of the VTP domain. Therefore, your recently−introduced switch, with almost no configured VLANs, has erased all VLANs through the VTP domain.

This will happen whether the switch is a VTP client or a VTP server. A VTP client can erase VLAN information on a VTP server. You will know that this has happened when many of the ports in your network go into inactive state, but continue to be assigned to a non−existing VLAN.

Solution:

Quickly reconfigure all of the VLANs on one of the VTP servers.

What to Remember:

Always make sure that the configuration revision of all switches inserted into the VTP domain is lower than the configuration revision of the switches already in the VTP domain.

If you have the output of a **show tech−support** command from your Cisco device, you can use to display potential issues and fixes. To use, you must be a registered customer, be logged in, and have JavaScript enabled.

You can use Output Interpreter to display potential issues and fixes. To use Output Interpreter, you must be a registered customer, be logged in, and have JavaScript enabled.

Example:

For an example, follow these steps:

1. Clic has 7 VLANs (1, 2, 3, and, the defaults) and is the VTP server in domain test, port 2/3 is in VLAN 3:

```
clic (enable) show vlan
1993 May 25 05:09:50 %PAGP−5−PORTTOSTP:Port 2/1 joined bridge port 2/1 lan
VLAN Name                             Status    IfIndex Mod/Ports, Vlans
---- -------------------------------- --------- ------- ------------------------
1    default                          active    65      2/2,2/4−50
2    VLAN0002                         active    70
3    VLAN0003                         active    71      2/3
1002 fddi−default                     active    66
1003 token−ring−default               active    69
1004 fddinet−default                  active    67
1005 trnet−default                    active    68      68

clic (enable) show vtp domain
Domain Name                      Domain Index VTP Version Local Mode  Password
−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−− −−−−−−−−−−−− −−−−−−−−−−− −−−−−−−−−−− −−−−−−−−−−
test                             1            2           server      −

Vlan−count Max−vlan−storage Config Revision Notifications
−−−−−−−−−− −−−−−−−−−−−−−−−− −−−−−−−−−−−−−−− −−−−−−−−−−−−−
7          1023             0               disabled

Last Updater    V2 Mode  Pruning  PruneEligible on Vlans
−−−−−−−−−−−−−−− −−−−−−−− −−−−−−−− −−−−−−−−−−−−−−−−−−−−−−−−−
0.0.0.0         disabled disabled 2−1000

clic (enable) show port 2/3
Port  Name               Status     Vlan       Level  Duplex Speed Type
−−−−− −−−−−−−−−−−−−−−−−− −−−−−−−−−− −−−−−−−−−− −−−−−− −−−−−− −−−−− −−−−−−−−−−−−
 2/3                     connected 3          normal   10  half 10/100BaseTX
```

2. Connect Bing (which is a lab switch on which VLAN 4, 5 and 6 were created).

Note that the configuration revision is 3 in this switch:

```
bing (enable) show vlan
VLAN Name                             Status    IfIndex Mod/Ports, Vlans
−−−− −−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−− −−−−−−−−− −−−−−−− −−−−−−−−−−−−−−−−−−−−−−−−
1    default                          active    4       2/1−48
                                                        3/1−6
4    VLAN0004                         active    63
5    VLAN0005                         active    64
6    VLAN0006                         active    65
1002 fddi−default                     active    5
1003 token−ring−default               active    8
1004 fddinet−default                  active    6
1005 trnet−default                    active    7
```

3. Then, place Bing in the same VTP domain test:

```
bing (enable) show vtp domain
Domain Name                      Domain Index VTP Version Local Mode  Password
−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−− −−−−−−−−−−−− −−−−−−−−−−− −−−−−−−−−−− −−−−−−−−−−
test                             1            2           server      −

Vlan−count Max−vlan−storage Config Revision Notifications
−−−−−−−−−− −−−−−−−−−−−−−−−− −−−−−−−−−−−−−−− −−−−−−−−−−−−−
8          1023             3               disabled

Last Updater    V2 Mode  Pruning  PruneEligible on Vlans
−−−−−−−−−−−−−−− −−−−−−−− −−−−−−−− −−−−−−−−−−−−−−−−−−−−−−−−−
10.200.8.38     disabled disabled 2−1000
```

4. Then, configure the trunk between the two switches in order to integrate Bing in the network.

   Notice that Bing erased the Clic VLAN, and now Clic has VLAN 4, 5, 6. However, it no longer has 2 and 3, and port 2/3 is inactive:

```
clic (enable) show vtp domain
Domain Name                      Domain Index VTP Version Local Mode  Password
−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−− −−−−−−−−−−−− −−−−−−−−−−− −−−−−−−−−−− −−−−−−−−−−
test                             1            2           server      −

Vlan−count Max−vlan−storage Config Revision Notifications
−−−−−−−−−− −−−−−−−−−−−−−−−− −−−−−−−−−−−−−−− −−−−−−−−−−−−−
8          1023             3               disabled

Last Updater    V2 Mode  Pruning  PruneEligible on Vlans
−−−−−−−−−−−−−−− −−−−−−−− −−−−−−−− −−−−−−−−−−−−−−−−−−−−−−−−−
10.200.8.38     disabled disabled 2−1000
clic (enable)
clic (enable)
clic (enable) show vlan
VLAN Name                             Status    IfIndex Mod/Ports, Vlans
−−−− −−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−− −−−−−−−−− −−−−−−− −−−−−−−−−−−−−−−−−−−−−−−−
1    default                          active    65      2/2,2/4−50
4    VLAN0004                         active    72
5    VLAN0005                         active    73
6    VLAN0006                         active    74
1002 fddi−default                     active    66
```

```
1003 token-ring-default               active    69
1004 fddinet-default                  active    67
1005 trnet-default                    active    68      68

clic (enable) show port 2/3
Port  Name               Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------------
 2/3                     inactive   3          normal   auto  auto 10/100BaseTX
```

Resetting the Configuration Revision

You can easily reset the configuration revision number by replacing the new domain name with the original domain name:

1. The configuration is empty:

```
clic (enable) show vtp domain
Domain Name                      Domain Index VTP Version Local Mode  Password
-------------------------------- ------------ ----------- ----------- ----------
                                 1            2           server      -

Vlan-count Max-vlan-storage Config Revision Notifications
---------- ---------------- --------------- -------------
5          1023             0               disabled

Last Updater    V2 Mode  Pruning  PruneEligible on Vlans
--------------- -------- -------- -------------------------
0.0.0.0         disabled disabled 2-1000
clic (enable)
```

2. In this example, the domain "test" is configured and two VLANS are created.

   The configuration revision goes up to 2:

```
clic (enable) set vtp domain test
VTP domain test modified
clic (enable)
clic (enable) set vlan 2
Vlan 2 configuration successful
clic (enable) set vlan 3
Vlan 3 configuration successful
clic (enable) sh vtp domain
Domain Name                      Domain Index VTP Version Local Mode  Password
-------------------------------- ------------ ----------- ----------- ----------
test                             1            2           server      -

Vlan-count Max-vlan-storage Config Revision Notifications
---------- ---------------- --------------- -------------
7          1023             2               disabled

Last Updater    V2 Mode  Pruning  PruneEligible on Vlans
--------------- -------- -------- -------------------------
0.0.0.0         disabled disabled 2-1000
clic (enable)
```

3.

Change the domain name from "test" to "cisco".

The configuration revision is back to 0 and all of the VLANs are still present:

```
clic (enable) set vtp domain cisco
VTP domain cisco modified
clic (enable) show vtp domain
Domain Name                      Domain Index VTP Version Local Mode  Password
−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−− −−−−−−−−−−−− −−−−−−−−−−− −−−−−−−−−−− −−−−−−−−−−
cisco                            1            2           server      −

Vlan−count Max−vlan−storage Config Revision Notifications
−−−−−−−−−− −−−−−−−−−−−−−−−− −−−−−−−−−−−−−−− −−−−−−−−−−−−−
7          1023             0               disabled

Last Updater    V2 Mode  Pruning  PruneEligible on Vlans
−−−−−−−−−−−−−−− −−−−−−−− −−−−−−−− −−−−−−−−−−−−−−−−−−−−−−−−−
0.0.0.0         disabled disabled 2−1000
```

4.
   Change the VTP domain name from "cisco" back to "test".

   The configuration revision is 0. There is no risk that anything will be erased, and all the previously configured VLANs remain:

```
clic (enable) set vtp domain test
VTP domain test modified
clic (enable) show vtp domain
Domain Name                      Domain Index VTP Version Local Mode  Password
−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−− −−−−−−−−−−−− −−−−−−−−−−− −−−−−−−−−−− −−−−−−−−−−
test                             1            2           server      −

Vlan−count Max−vlan−storage Config Revision Notifications
−−−−−−−−−− −−−−−−−−−−−−−−−− −−−−−−−−−−−−−−− −−−−−−−−−−−−−
7          1023             0               disabled

Last Updater    V2 Mode  Pruning  PruneEligible on Vlans
−−−−−−−−−−−−−−− −−−−−−−− −−−−−−−− −−−−−−−−−−−−−−−−−−−−−−−−−
0.0.0.0         disabled disabled 2−1000
clic (enable)
```

Trunk Down Causing VTP Problems

Remember, VTP packets are carried on VLAN 1, but only on trunks (ISL, dot1Q or LANE).

If you make VLAN changes during a time when you have a trunk down or LANE−connectivity down between two parts of your network, you may lose your VLAN configuration. When the trunk connectivity is restored, the two sides of the network will resynchronize. Therefore, the switch with the highest configuration revision will erase the VLAN configuration of the lowest configuration revision switch.

VTP and Spanning Tree Protocol (Logical Spanning Tree Port)

Be aware that when you have a large VTP domain, you will also have a large Spanning−Tree Protocol (STP) domain. VLAN 1 must span through the whole VTP domain. Therefore, one unique STP is run for that VLAN in the whole domain.

When VTP is used and a new VLAN is created, the VLAN is propagated through the entire VTP domain. The VLAN is then created in all switches in the VTP domain. All Cisco switches use Per−VLAN Spanning Tree (PVST), which means that they are running a separate STP for each VLAN, which is adding to the CPU load of the switch. To have an idea on the number of STPs that you can have on each switch, you need to refer to the maximum number of logical ports (for the STP) supported on the switch. The number of logical ports is roughly the amount of ports running STP (knowing that a trunk port will be running one instance of STP per the active VLAN on the trunk). A rapid evaluation of this value for your switch can be found by using the following formula:

- [(Number of active VLAN x Number of trunk)+ Number of access port]

This number (maximum number of logical ports for STP) varies from switch to switch, and is documented in the release notes of each product. For example, on a Catalyst 5000 with a Sup2, you can have a maximum of 1500 STP instances. Keep in mind that each time you create a new VLAN with VTP, this VLAN will be propagated by default to all switches, and will be active on all ports. To avoid having the number of logical ports blowing up, you may need to consider pruning unnecessary VLANs from the trunk. This can be done by using VTP pruning.

VTP Pruning

VTP pruning is the manual pruning of the VLAN from the trunk using the **clear trunk mod/port** and **clear trunk vlan_list** commands. For example, only allow on each trunk a core switch to the VLANS that are actually needed. This is the advantage to reducing the load on the CPU of all switches (core switches and access switches), and to avoid having the STP for those VLANs to extend through the entire network. This will limit STP problems in the VLAN.

For example:

- Topology: Two core switches connected to each, both having 80 trunk connections to 80 different access switches. With this design, each core switch will have 81 trunks, and each access switch will have two uplink trunks, assuming that access switches have (in addition to the two uplinks) two or three trunks going to a small Catalyst 1900. This is a total of four to five trunks per access switch.
- Platform: Core switches are Catalyst 6500s with Sup1A and PFC1 running Cisco IOS software 5.5(7). According to the release notes, this platform cannot have more than 4000 STP logical ports.
- Access switches are either: Catalyst 5000s with Sup2 who do not support more than 1500 STP logical ports, or Catalyst 5000s with Sup1 and 20 M of DRAM, which do not support more than 400 STP logical ports.
- Number of VLANs: Remember to use VTP, a VLAN on the VTP server will be created on all switches in the network. If we have 100 VLANs, the core will handle roughly (100 VLANs x 81 trunks)= 8100 logical ports (above the limit), and the access switch will handle (100 VLANs x 5 trunks)= 500 logical ports. Catalysts in the core will be above their supported number of logical ports, and access switches with Sup1 will also be above the limit.
-

Solution: If it is assumed that only four or five VLANs are actually needed in each access switch, you can prune all other VLANs from the trunk on the core layer. For example, if only VLANs 1, 10, 11, and 13 are needed on trunk 3/1 going to that access switch, the configuration is as follows on the core:

```
Praha> (enable) set trunk 1/1 des
Port(s) 1/1 trunk mode set to desirable.
Praha> (enable) clear trunk 1/1 2−9,12,14−1005
Removing Vlan(s) 2−9,12,14−1005 from allowed list.
Port 1/1 allowed vlans modified to 1,10,11,13.
Praha> (enable) clear trunk 1/1 2−9,12,14−1005
```

Note: Even if you do not exceed the number of allowed logical ports, pruning VLANs from a trunk is recommended for the following reason:

- A STP loop in one VLAN will only extend where the VLAN is allowed, and will not go through the entire campus. The broadcast in one VLAN will not reach the switch that does not need the broadcast. Before Cisco IOS software release 5.4, you could not clear VLAN 1 from trunks. Now, you can clear VLAN 1 by issuing the following command:

```
Praha> (enable) clear trunk 1/1 1
Default vlan 1 cannot be cleared from module 1.
```

In the following section, techniques will be discussed on how to avoid VLAN 1 spanning the whole campus.

The Case of VLAN 1

VTP pruning cannot be applied to VLANs that need to exist everywhere and to be allowed on all switches in the campus (to be able to carry VTP, CDP traffic, and other control traffic). There is a way, however, to limit the extent of VLAN 1. This is a feature called **VLAN 1 disable on trunk**, and it is available on Catalyst 4000, 5000, and 6000 family switches since Cisco IOS release 5.4(x). This allow you to prune VLAN 1 from a trunk as you would do for any other VLAN, but this pruning will not include all of the control protocol traffic that will still be allowed on the trunk (DTP, PagP, CDP, VTP, and so on). However, you will block all user traffic on that trunk. Using this feature, you can completely avoid the VLAN spanning the entire campus, and as such, STP loops will be limited in extent, even in VLAN 1. You can configure VLAN 1 to be disabled as you would configure other VLANs to be cleared from the trunk by issuing the following commands:

```
Console> (enable) set trunk 2/1 Des
Port(s)  2/1 trunk mode set to desirable.
Console> (enable) clear trunk 2/1 1
Removing Vlan(s) 1 from allowed list.
Port  2/1 allowed vlans modified to 2−1005.
```

CatOS Switch Changes to VTP Transparent Mode, VTP−4−UNSUPPORTEDCFGRCVD:

A recent change in CatOS incorporated a protective feature that causes a CatOS switch to go into VTP Transparent mode in order to prevent the possibility of a switch reset due to a Watch Dog Timeout. This change is documented in CSCdu32627.

How do I determine whether my switch might be affected?

The Watch Dog Timeout can occur if the following two conditions are met:

- The Token Ring VLAN (1003) is translated to VLAN 1.
- You make a change in VLAN 1.

To observe the Token Ring VLAN translation, perform a **show vlan** command in the Catalyst. Example **show vlan** command output is presented below:

```
VLAN Type  SAID       MTU   Parent RingNo BrdgNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ ------ ---- -------- ------ ------
1    enet  100001     1500  -      -      -      -    -        1003
```

How does CatOS Version 6.3(3) protect my switch from having a Watch Dog Timeout?

The protective feature for preventing a Watch Dog Timeout is for the Catalyst to switch from VTP Server/Client to VTP Transparent mode.

How do I determine whether my switch has gone to VTP Transparent mode to protect from a Watch Dog Timeout?

Your switch has gone to VTP Transparent mode if the logging level for the VTP is raised to 4.

```
Console> (enable) set logging level vtp 4 default
```

You see the following message when the switchover occurs:

VTP−4−UNSUPPORTEDCFGRCVD:Rcvd VTP advert with unsupported vlan config on trunk mod/port− VTP mode changed to transparent

What are the negative effects from the switch going to VTP Transparent mode?

1. If pruning is enabled, the trunks will go down.
2. If trunks go down and no other ports are in that VLAN, the VLAN interface in the installed Multilayer Switch Feature Card (MSFC) will go down.

If the effects described above occur, your network could be negatively affected if, for example, this switch is in the core of your network.

Where does the unsupported VTP configuration come from?

Any Cisco IOS−based switch, such as a Catalyst 2900/3500XL, a Native Mode Catalyst 6500 or an Cisco IOS−based Catalyst 4000, can supply the unsupported VTP configuration because these products translate the 1003 VLAN to VLAN 1 by default.

What Is the Solution?

The solution in Catalyst OS−based switches enables the switches to handle this translated information properly. The solution for the IOS−based switches is to remove this default translation and match the Catalyst OS−based switches' behavior. The integrated fixed versions are available currently as follows:

Catalyst Switch	Fixed Releases
Catalyst OS switches	5.5(14) and later 6.3(6) and later 7.2(2) and later
Catalyst 4000 Supervisor III	Not Affected
Catalyst 6500 (Supervisor IOS)	12.1(8a)EX and later
Catalyst 2900 and 3500 XL	12.0(5)WC3 and later

If it is not possible to upgrade to images that have these bugs integrated, the configuration can be modified in the Cisco IOS−based switches with the following procedure if the switch is a VTP server.

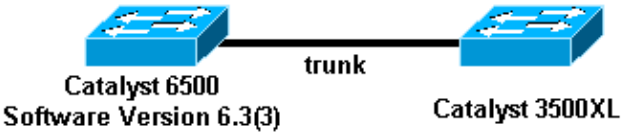
```
goss# vlan data
goss(vlan)#no vlan 1 tb−vlan1 tb−vlan2
Resetting translation bridge VLAN 1 to default
Resetting translation bridge VLAN 2 to default
goss(vlan)#no vlan 1003 tb−vlan1 tb−vlan2
Resetting translation bridge VLAN 1 to default
Resetting translation bridge VLAN 2 to default
goss(vlan)#apply
APPLY completed.
goss(vlan)#exit
APPLY completed.
Exiting....
```

The 1002 VLAN can be translated, but it may also be removed if you include the following in your configuration:

```
goss(vlan)#no vlan 1002 tb−vlan1 tb−vlan2
Resetting translation bridge VLAN 1 to default
Resetting translation bridge VLAN 2 to default
```

When exactly will my switch change to VTP Transparent mode?

Some confusion exists concerning when this switchover to VTP Transparent Mode occurs. The following scenarios are examples of when we have observed it happen:



Example 1

Initial conditions:

-

Both the Catalyst 6500 and the Catalyst 3500XL are VTP servers with the same VTP configuration revision.

- Both have the same VTP domain name and the same VTP password, if configured.
- The Catalyst 3500XL has the translated TR−VLAN.
- Start with them disconnected.

If you connect these two, the Catalyst 6500 goes to VTP Transparent mode. Of course, this also happens if the Cisco 3500XL has a higher VTP configuration revision. Moreover, if the switch to VTP Transparent mode happens when you physically connect the two, it is reasonable to assume it would also happen if the Catalyst 6500 was booting up for the first time and it was already connected.

Example 2

Initial conditions:

- The Catalyst 6500 is a VTP server.
- The Catalyst 3500XL is a VTP client.
- The Catalyst 3500XL has a higher VTP configuration revision.
- Both switches have the same VTP domain and the same VTP password, if configured.
- The Catalyst 3500XL has the translated TR−VLAN.
- Start with them disconnected.

If you connect these two, the Catalyst 6500 goes to VTP Transparent mode. In this scenario, if the Catalyst 3500XL has a lower configuration revision, the Catalyst 6500 does not switch to VTP transparent. If the Catalyst 3500XL has the same configuration revision, the Catalyst 6500 does not go to VTP Transparent mode, but the translation is still be present in the Catalyst 3500XL.

What is the quickest way to recover once I notice the translation in my network?

Even if you correct the TR−VLAN information in one switch, such as the one that was malfunctioning, the information might have propagated throughout your network. You can use the **show vlan** command to check this. Therefore, the quickest way to recover is to take a Cisco IOS−based switch, like a Catalyst XL that is connected to the network, change it to a VTP server, and remove the translated VLANs. Once you apply the change in that Catalyst XL, the change should be propagated to all the other VTP servers/clients once it is reconnected to the network. You can use the **show vlan** command to verify that the translation is gone in the network. At this point, it should be possible to change the affected CatOS 6.3(3) switch back to a VTP server.

Note: The Catalyst XL switches do not support as many VLANs as the Catalyst 6500s do, so you should take care to ensure that all of the VLANs in the Catalyst 6500 exist in the Catalyst XL switch before reconnecting them. For example, you would not want to connect a Catalyst 3548 XL with 254 VLANs with a higher VTP configuration revision to your Catalyst 6500 that has 500 VLANs configured.

Troubleshooting VTP Configuration Revision Number Errors Seen in the show vtp statistics Command

VTP is designed for an administrative environment in which the domain's VLAN database is changed at only one switch at any one time, and assumes that the new revision will propagate throughout the domain before another revision is made. Changing the database simultaneously on two different devices in the administrative domain can result in two different databases being generated with the same revision number propagating and overwriting the existing information until they meet at an intermediate catalyst switch on the network. This switch cannot accept either advertisement because the packets have the same revision number but a different MD5 digest value. When it detects this condition, the switch increments the "No of config revision errors" counter. If you encounter a problem such as the VLAN information is not updated on a certain switch, issue the **show vtp statistics** command to check if the count of VTP packets with configuration revision number errors is increasing, as shown in the following example:

```
Console> (enable) show vtp statistics

VTP statistics:
summary advts received          4690
subset  advts received          7
request advts received          0
summary advts transmitted       4397
subset  advts transmitted       8
request advts transmitted       0
No of config revision errors    5
No of config digest errors      0
VTP pruning statistics:
Trunk     Join Trasmitted  Join Received  Summary advts received from
                                          non−pruning−capable device
−−−−−−−−  −−−−−−−−−−−−−−−  −−−−−−−−−−−−−  −−−−−−−−−−−−−−−−−−−−−−−−−−−
 1/1      0                0              0
 1/2      0                0              0
Console> (enable)
```

If you observe a configuration revision error, you can resolve this problem by changing the VLAN database in some way so that a VTP database with a higher revision number than the competing databases is created. For example, on the switch acting as the primary VTP server, add or delete a bogus VLAN in the administrative domain. This updated revision will be propagated throughout the domain, overwriting the database at all devices. With all of the devices in the domain advertising identical databases, the error no longer will appear.

Troubleshooting VTP Configuration Digest Errors Seen in the show vtp statistics Command

This section addresses troubleshooting VTP configuration digest errors seen from issuing the **show vtp statistics** command, as shown in the following example:

```
Console> (enable) show vtp statistics

VTP statistics:
```

```
summary advts received          3240
subset  advts received          4
request advts received          0
summary advts transmitted       3190
subset  advts transmitted       5
request advts transmitted       0
No of config revision errors    0
No of config digest errors      2
VTP pruning statistics:
Trunk     Join Trasmitted  Join Received  Summary advts received from
                                          non−pruning−capable device
−−−−−−−−  −−−−−−−−−−−−−−−  −−−−−−−−−−−−−  −−−−−−−−−−−−−−−−−−−−−−−−−−−
 1/1      0                0              0
 1/2      0                0              0
Console> (enable)
```

The general purpose of an MD5 value is to verify the integrity of a received packet, and to detect any changes or corruption to the packet during transit. When a switch detects a new revision number different from the currently stored value, it sends a request message to the VTP server and requests the VTP subsets. A subset advertisement contains a list of VLAN information. The switch calculates the MD5 value for the subset advertisement(s) and compares it to the MD5 value of the VTP summary advertisement. If the two values are different, the switch increases the "No of config digest errors" counter.

A common reason for these digest errors is that the VTP password is not configured consistently on all VTP servers in the VTP domain. Troubleshoot these errors as a misconfiguration or data corruption issue.

Make sure that when troubleshooting this problem the error counter is not historical. The statistics menu counts errors since the device reset or the VTP statistics reset.

Conclusion

There are some disadvantages to using VTP. You must balance the VTP's ease of administration with the risk of a large STP domain, and all the potential instability and risks linked with STP. The greatest risk would be a STP loop through the entire campus. When using VTP, there are two things you need to pay close attention to:

- Remember the configuration revision and how to reset each time you insert a new switch in your network to avoid bringing down the entire network.
- As much as possible, avoid having a VLAN that spans the entire network.

Related Information

- **Technical Support − Cisco Systems**

Updated: Dec 17, 2002 Document ID: 10558