Table of Contents

Understanding and Configuring VLAN Trunk Protocol (VTP)

Document ID: 10558

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

This document contains Flash animation.

Introduction

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 to configure the same VLAN everywhere. VTP is a Cisco−proprietary protocol that is available on most of the Cisco Catalyst Family products.

Note: This document does not cover VTP Version 3. VTP Version 3 differs from VTP Versions 1 and 2, and it is only available on CatOS 8.1(1) or later. VTP Version 3 incorporates many changes from VTP Versions 1 and 2. Make certain that you understand the differences between VTP Version 3 and prior versions before you alter your network s configuration. For more information, refer to Understanding How VTP Version 3 Works or VTP Version 3 Interaction with VTP Version 1 and VTP Version 2.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

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

Conventions

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

Understanding VTP

Flash animation: VTP

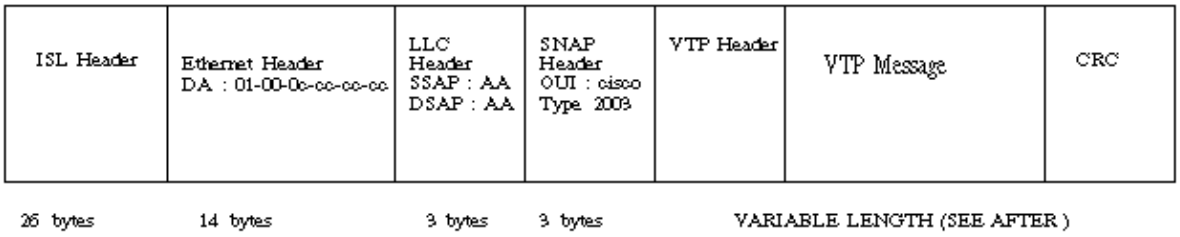

Refer to the VTP Flash animation which explains these concepts for VTP Versions 1 and 2:

- Introduction to VTP
- VTP Domain and VTP Modes
- Common VTP Problems and Solutions

Note: This document does not cover VTP Version 3. VTP Version 3 differs from VTP Versions 1 and 2 and is only available on CatOS 8.1(1) or later. For more information, refer to Understanding How VTP Version 3 Works or VTP Version 3 Interaction with VTP Version 1 and VTP Version 2.

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). This 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 consider the detail of a VTP packet. The format of the VTP header can vary based on the type of VTP message. However, they all contain these fields in the header:

- VTP protocol version: 1, 2, or 3
- 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 the VTP configuration revision number that is assigned to it, and most of the VTP packets contain the VTP configuration revision number of the sender.

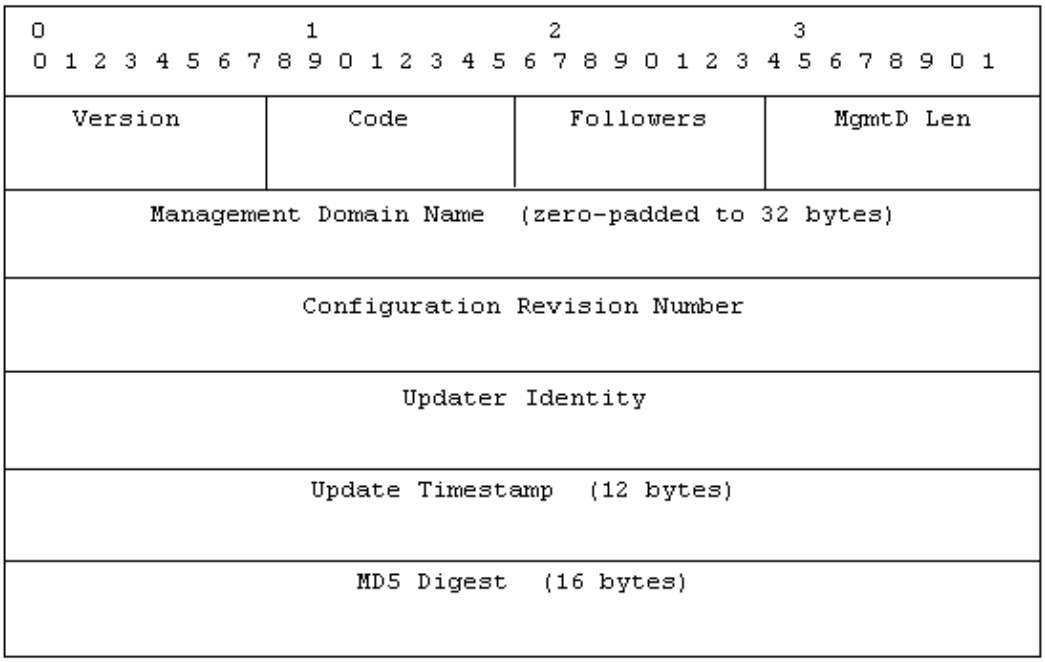
This information is used to determine whether the received information is more recent than the current version. Each time you make a VLAN change in a VTP device, the configuration revision is incremented by one. To reset the configuration revision of a switch, change the VTP domain name and then change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

Summary Advertisements

By default, Catalyst switches 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 to its own 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 to its own 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:



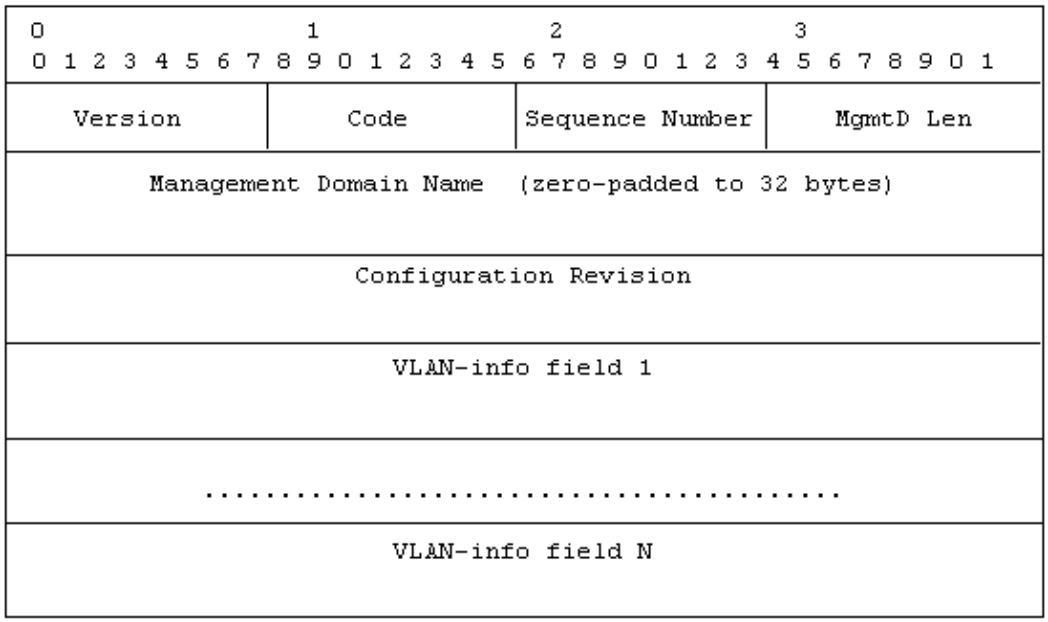
This list clarifies the meaning of those fields in the summary advertisement packet:

- Followers indicate that this packet is followed by a Subset Advertisement packet.
- The updater identity is the IP address of the switch that is the last to have 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.

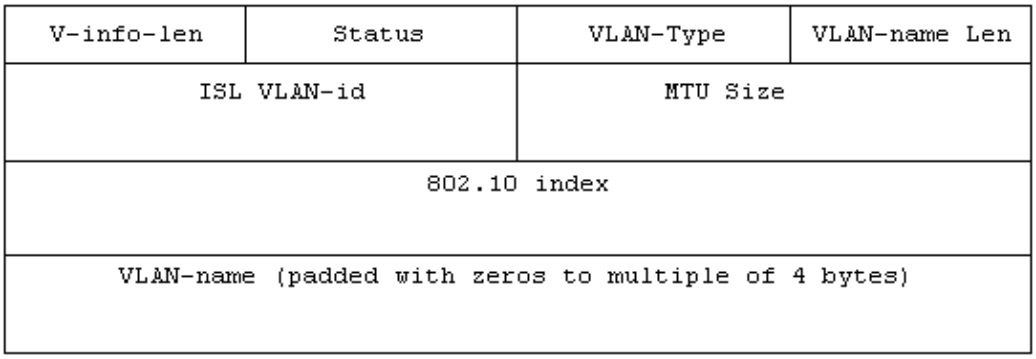
Subset Advertisements

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 to advertise them all.

Subset Advert Packet Format:



This formatted example shows that each VLAN information field contains information for a different VLAN (ordered so that lowered−valued ISL VLAN IDs occur first):



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

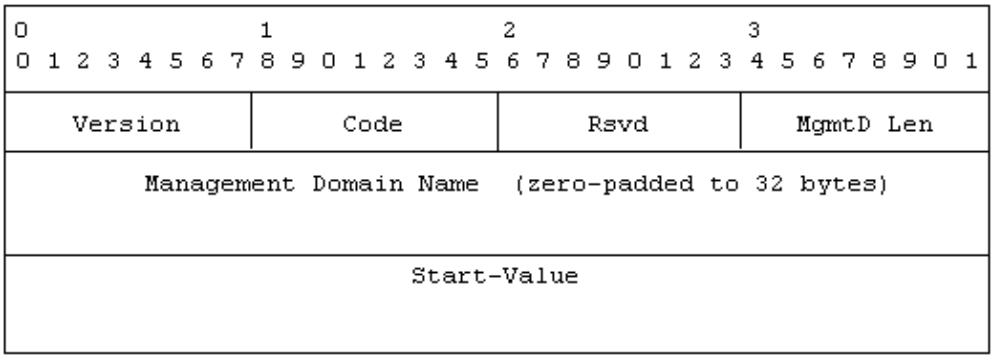
- **Code** The format for this is 0x02 for subset advertisement.
- **Sequence number** This is the sequence of the packet in the stream of packets that follow a summary advertisement. The sequence starts with 1.

Advertisement Requests

A switch needs a VTP advertisement request in these 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. This is an example:



- **Code** The format for this is 0x03 for an advertisement request.
- **Start Value** This is 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, then the Catalyst only requests advertisements from the (*n*+1)th one.

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 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, then it needs to be configured on all switches in the VTP domain, and it needs to be the same password on all of those switches. The VTP password that you configure is translated by algorithm into a 16−byte word (MD5 value) that is carried in all summary−advertisement VTP packets.

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 over the entire 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 (or *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 is small and is easily stored in all switches (in NVRAM). In a large network, a judgment call must be made at some point, when the NVRAM storage that is needed is wasteful because it is duplicated on every switch. At this point, the network administrator should choose a few well−equipped switches and keep them as VTP servers. Everything else that participates in VTP can be turned into a client. The number of VTP servers should be chosen to provide the degree of redundancy that is desired in the network.

Notes:

- If a switch is configured as a VTP server without a VTP domain name, you can not configure a

VLAN on it.
- If a new Catalyst is attached in the border of two VTP domains, the new Catalyst keeps 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.
- Dynamic Trunk Protocol (DTP) sends the VTP domain name in a DTP packet. Therefore, if you have two ends of a link that belong to different VTP domains, then the trunk does not come up if you use DTP. In this special case, you need to configure the trunk mode as `on` or `nonegotiate`, on both sides, to allow the trunk to come up without DTP negotiation agreement.

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 that are found on other Catalyst switches (such as VTP, DTP, and Point Aggregation Protocol [PAgP]).

Catalyst 6000 Family Cisco IOS System Software / Catalyst 4000 Cisco IOS (Supervisor III/Supervisor IV), Cat2950, 3550, and 3750 Series Switches

There are two methods that you can use to configure VTP, as shown in this section. (The second method is not available in older software on Catalyst 6500 series switches that run Cisco IOS® software.)

1. **In VLAN database mode:**

   In Cisco IOS software, you can configure the VTP domain name, the VTP mode, and the VLANs in VLAN configuration mode.

   a. In the exec mode, issue this command to enter VLAN configuration mode:

```
Router# vlan database

!--- This command is issued in Privileged EXEC mode,
!--- not in global configuration mode.

Router(vlan)#

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

   b. To set the VTP domain name, issue this command:

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

   c. To exit VLAN configuration mode use, issue the **exit** command; the **end** command and **Ctrl−Z** keys do not work in this mode.

```
Router(vlan)# end

Router(vlan)# ^Z

% Invalid input detected at '^' marker.

Router(vlan)#

Router(vlan)# exit
```

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

2. **In Global configuration mode:**

   In Cisco IOS software global configuration mode, all VTP parameters can be configured by Cisco IOS software commands. This is the command format:

```
Router(config)# vtp ?

domain     Set the name of the VTP administrative domain.
file       Configure IFS filesystem file where VTP configuration is stored.
interface  Configure interface as the preferred source for the VTP IP updater
           address.
mode       Configure VTP device mode
password   Set the password for the VTP administrative domain
pruning    Set the administrative domain to permit pruning
version    Set the administrative domain to VTP version
```

3. To monitor VTP operation and status, issue these commands:

```
Router# show vtp status

Router# show vtp counters
```

Catalyst 4000, 5000, or 6000 Family CatOS

To set the domain name:

```
set vtp domain name
```

To set the mode:

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

To monitor the VTP operation and status:

```
show vtp domain
show vtp status
```

Catalyst 2900XL, 3500XL, 2950, and 3550

From the VLAN database mode (similar to Cisco 6500 series that run Cisco IOS software), issue these commands:

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

From the Enable mode, issue these commands to monitor VTP operation:

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

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

Catalyst 2900XL series switches.

Practical Examples

This first example involves two Catalyst 4000 switches that are connected by a Fast Ethernet 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 the VTP domain test.
2. In this sample output from the **show vtp domain** command, you can see that the VTP version is set at 2. This means that the switch is VTP V2 capable; but it does not run VTP V2 in this case. It only runs VTP V2 if the V2 mode is enabled with the **set vtp v2 enable** command:

```
bing (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
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 domain

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. At this stage, 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 (in Frame 1 in this sample output):

```
!--- On bing:

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

!--- This indicates that bing has received its
!--- first summary advertisement.

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

!--- This is where bing gets the 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 (in Frame 2 in this sample output):

```
!--- On bing:

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

!--- This is where the advertisement 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 that contains all VLANs (in Frame 3 in this output). 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

!--- Bing has received its second summary advertisement.

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

!--- This configuration revision is higher than that on bing.

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

!--- Bing has received its subset advertisement.

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 are the numbers.

      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 domain

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
```

This example shows how to verify the VTP configuration on a Catalyst 6000 that is running Cisco IOS software:

```
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#
```

This example shows how to display VTP statistics on a Catalyst 6000 that is running Cisco IOS software:

```
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

This section discusses some common troubleshooting situations for VTP.

How a Recently Inserted Switch Can Cause Network Problems

Note: To see a Flash demonstration of this problem, refer to the Understanding VTP section.

This problem occurs when you have a large switched domain that 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 was 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 happens whether the switch is a VTP client or a VTP server. A VTP client can erase VLAN information on a VTP server. You can tell that this has happened when many of the ports in your network go into inactive state but continue to be assigned to a nonexistent 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 that you insert into the VTP domain is lower than the configuration revision of the switches that are already in the VTP domain.

If you have the output of a **show tech−support** command from your Cisco device, you can use Output Interpreter (registered customers only) to display potential issues and fixes.

Example

Follow these steps to see an example of this problem:

1. Clic has 7 VLANs (1, 2, 3, and the defaults) and is the VTP server in the domain named 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 VLANs 4, 5, and 6 were created.

   Note: 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. 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. Configure the trunk between the two switches, to integrate bing in the network.

   Bing erased the Clic VLAN, and now Clic has VLANs 4, 5, and 6. However, it no longer has VLANs 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) 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. Replace 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 named 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) set vlan 2

Vlan 2 configuration successful

clic (enable) set vlan 3

Vlan 3 configuration successful

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             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 of 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)
```

All Ports Inactive After Power Cycle

Switch ports move to the inactive state when they are members of VLANs that do not exist in the VLAN database. A common issue is that all of the ports move to this inactive state after a power cycle. Generally, you see this when the switch is configured as a VTP client with the uplink trunk port on a VLAN other than VLAN 1. Because it is in VTP client mode, when the switch resets, it loses its VLAN database and causes the uplink port and any other ports that were not members of VLAN 1 to go into inactive mode. To solve this problem, follow these steps:

1. Temporarily change the VTP mode to transparent.

```
switch (enable) set vtp mode transparent

VTP domain austinlab modified
```

```
switch (enable)
```

2. Add the VLAN to which the uplink port is assigned to the VLAN database. (This example assumes that VLAN 3 is that VLAN which is assigned to the uplink port.)

```
switch (enable) set vlan 3

VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 3 configuration successful
switch (enable)
```

3. Change the VTP mode back to client, after the uplink port begins forwarding.

```
switch (enable) set vtp mode client

VTP domain austinlab modified
```

After you follow those steps, VTP should repopulate the VLAN database from the VTP server, and thus move all ports back into the active state that were members of VLANs advertised by the VTP server.

Trunk Down Causing VTP Problems

Remember, VTP packets are carried on VLAN 1, but only on trunks (ISL, dot1q, or LANE [LAN emulation]).

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 resynchronize. Therefore, the switch with the highest configuration revision erases the VLAN configuration of the lowest configuration revision switch.

VTP and Spanning Tree Protocol (Logical Spanning Tree Port)

When you have a large VTP domain, you 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 of the number of STPs that you can have on each switch, you must refer to the maximum number of logical ports (for the STP) supported on the switch. The number of logical ports is roughly the number of ports running STP (a trunk port is running one instance of STP for each active VLAN on the trunk). A rapid evaluation of this value for your switch can be found with this formula:

```
(Number of active VLANs × Number of trunks) + Number of access ports
```

This number (the maximum number of logical ports for STP) varies from switch to switch, and is documented in the release notes for 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 is propagated by default to all switches and is subsequently active on all ports. To avoid inflation of the number of logical ports, you may need to consider pruning unnecessary VLANs from the trunk. This can be done with VTP pruning.

Note: Pruning unnecessary VLANs from the trunk can be done with one of two methods:

1. **Manual pruning of the unnecessary VLAN on the trunk** This is the best method, and it avoids the use of the spanning tree. Instead, it runs the pruned VLAN on trunks. Manual pruning is further described in the next section.
2. **VTP pruning** This method should be avoided, if the goal is to reduce the number of STP instances. VTP−pruned VLANs on a trunk are still part of the spanning tree, and thus do not reduce the number of spanning tree port instances.

VTP Pruning

VTP pruning is the manual pruning of the VLAN from the trunk with the **clear trunk *mod*/*port*** and **clear trunk *vlan_list*** commands. For example, you can choose to only allow, on each trunk, a core switch to the VLANs that are actually needed. This helps to reduce the load on the CPUs of all switches (core switches and access switches) and avoids the use of STP for those VLANs that extend through the entire network. This limits STP problems in the VLAN.

For example:

- **Topology** The topology is two core switches connected to each other, each with 80 trunk connections to 80 different access switches. With this design, each core switch has 81 trunks, and each access switch has two uplink trunks, assuming that access switches have (in addition to the two uplinks) two or three trunks that go to a 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 Release 5.5(7). According to the release notes, this platform can not have more than 4000 STP logical ports.
- **Access switches** Access switches are either Catalyst 5000s with Sup2 that do not support more than 1500 STP logical ports, or Catalyst 5000s with Sup1 and 20 MB 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 is created on all switches in the network. If we have 100 VLANs, the core must handle roughly 100 VLANs × 81 trunks = 8100 logical ports (above the limit), and the access switch must handle 100 VLANs × 5 trunks = 500 logical ports. Catalysts in the core would be above their supported number of logical ports, and access switches with Sup1 would 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 of the 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, this is the configuration 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, it is recommended that you prune VLANs from a trunk for this reason:

- ♦ An STP loop in one VLAN only extends where the VLAN is allowed and does not go through the entire campus. The broadcast in one VLAN does 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 with this command:

```
Praha> (enable) clear trunk 1/1 1

Default vlan 1 cannot be cleared from module 1.
```

In the next section, techniques are discussed on how to keep VLAN 1 from spanning the whole campus.

The Case of VLAN 1

VTP pruning can not be applied to VLANs that need to exist everywhere and that need 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 series switches in Cisco CatOS Release 5.4(x) and later. This allows you to prune VLAN 1 from a trunk as you would do for any other VLAN, but this pruning does not include all of the control protocol traffic that is still allowed on the trunk (DTP, PAgP, CDP, VTP, and so forth). However, it does block all user traffic on that trunk. With this feature, you can keep the VLAN from spanning the entire campus; and, as such, STP loops are limited in extent, even in VLAN 1. Configure VLAN 1 to be disabled as you would configure other VLANs to be cleared from the trunk:

```
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 Cisco bug IDs CSCdu32627 (registered customers only) and CSCdv77448 (registered customers only) .

How do I determine whether my switch might be affected?

The Watch Dog Timeout can occur if these 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. This is example **show vlan** command output:

```
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 to prevent a Watch Dog Timeout is for the Catalyst switch 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 against 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 this 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 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) goes down.

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

From where does the unsupported VTP configuration come?

Any Cisco IOS software−based switch (such as a Catalyst 2900/3500XL, a Cisco IOS software Catalyst 6500, or a Cisco IOS software−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 Cisco IOS software−based switches is to remove this default translation and match the behavior of the Catalyst OS−based switches. These are the integrated fixed versions that are currently available:

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 fixes integrated, the configuration can be modified in

the Cisco IOS software−based switches with this 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....
```

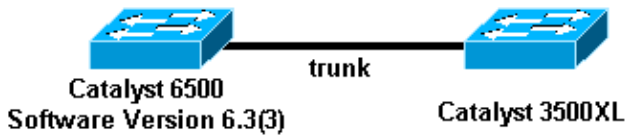
The 1002 VLAN can be translated, but it may also be removed if you include this in your configuration:

```
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 about when this switchover to VTP Transparent mode occurs. These scenarios are examples of when it can happen:



Example 1

Initial conditions:

- Both the Catalyst 6500 and the Catalyst 3500XL are VTP servers with the same VTP configuration revision.
- Both servers have the same VTP domain name and the same VTP password, if the password is configured.
- The Catalyst 3500XL has the translated TR−VLAN.
- The servers are started while 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 than the Catalyst 6500. 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 booted up for the first time while 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 than the Catalyst 6500.
- Both switches have the same VTP domain and the same VTP password, if the password is configured.
- The Catalyst 3500XL has the translated TR−VLAN.
- The servers are started while 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 than the Catalyst 6500, the Catalyst 6500 does not switch to VTP Transparent mode. 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 software−based switch (like a Catalyst XL that is connected to the network), change it to a VTP server, and remove the translated VLANs. When you have applied the change in that Catalyst XL and reconnected it to the network, the change should be propagated to all the other VTP servers and clients. 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 you reconnect them. For example, you would not want to connect a Catalyst 3548 XL with 254 VLANs and a higher VTP configuration revision to a 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 VLAN database for the domain is changed at only one switch at any one time; it assumes that the new revision propagates throughout the domain before another revision is made. If you change the database simultaneously on two different devices in the administrative domain, you can cause two different databases to be generated with the same revision number, which then propagate and overwrite the existing information until they meet at an intermediate Catalyst switch on the network. This switch can not 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 (see the next example output). If you find that the VLAN information is not updated on a certain switch, or if you encounter other, similar problems, then issue the **show vtp statistics** command to see if the count of VTP packets with configuration revision number errors is increasing:

```
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 if you change 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 that is acting as the primary VTP server, add or delete a false VLAN in the administrative domain. This updated revision is propagated throughout the domain and overwrites the database at all devices. When all of the devices in the domain advertise an identical database, the error no longer appears.

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

This section addresses troubleshooting VTP configuration digest errors that are seen when you issue the **show vtp statistics** command:

```
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 to the packet or corruption of the packet during transit. When a switch detects a new revision number that is 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.

When you troubleshoot this problem, ensure that the error counter is not historical. The statistics menu counts errors since the most recent device reset or the VTP statistics reset.

Conclusion

There are some disadvantages to the use of VTP. You must balance the ease of VTP administration against the inherent risk of a large STP domain and the potential instability and risks of STP. The greatest risk is an STP loop through the entire campus. When you use VTP, there are two things to which you need to pay close attention:

- Remember the configuration revision and how to reset it each time you insert a new switch in your network, so that you do not bring down the entire network.
- Avoid (as much as possible) having a VLAN that spans the entire network.

NetPro Discussion Forums − Featured Conversations

Related Information

- **LAN Product Support Pages**
- **LAN Switching Support Page**
- **Technical Support & Documentation − Cisco Systems**

Updated: Aug 10, 2005 Document ID: 10558