VTP Version 3

Introduction

Network administrators have to accommodate new and changing requirements on an ongoing base. They are faced with various, and often time-consuming, tasks like planning, implementing, expanding, and changing the network configuration. To make the most out of their precious available time, repetitive and error-prone tasks should be eliminated where possible. Two often-encountered tasks that can be optimized are the modification of the VLAN configuration and the MST (Multiple Spanning Tree) environment. Both tasks require the consistent modification of a group of devices. The effort required is directly proportional to the number of devices. Cisco Systems offers a unique and proven tool to optimize such tasks; VTP version 3 eases and secures the administration and the deployment in the field.

VTP version 3 is the third version of the VLAN trunk protocol and enhances its initial functions well beyond the handling of VLAN matters.

Key Benefits of VTP Version 3

Much work has gone into improving the usability of VTP version 3 in three major areas:

- The new version of VTP offers better administrative control over which device is allowed to update other devices' view of the VLAN topology. The chance of unintended and disruptive changes is significantly reduced, and availability is increased. The reduced risk of unintended changes will ease the change process and help speed deployment.
- Functionality for the VLAN environment has been significantly expanded. Two enhancements are most beneficial for today's networks:
  - In addition to supporting the earlier ISL VLAN range from 1 to 1001, the new version supports the whole IEEE 802.1Q VLAN range up to 4095.
  - In addition to supporting the concept of normal VLANs, VTP version 3 can transfer information regarding Private VLAN (PVLAN) structures.
- The third area of major improvement is support for databases other than VLAN (for example, MST).

VTP as a Layer 2 Messaging Protocol

VTP, as a Layer 2 signaling, control, or messaging protocol, is designed to simplify administration and to reduce unintended configuration errors. VTP is traditionally used to propagate information regarding VLANs such as additions, removals, state (active or suspended) or characteristic changes of VLANs. A characteristic change might be a change in the VLAN name (important for VLAN Membership Policy Server [VMPS]) in the MTU size. Because VTP is a Cisco protocol, it is easier for us to quickly adjust to today requirements. VTP provides services as needed by the customer and can be enhanced even further in the future. VTP usability has been enhanced for Cisco® Catalyst® 6500 IOS implementations (12.2(33)SXI) to support spanning tree, or more precisely the MST instance, to the VLAN mapping table with IOS. The initial manual configuration via CLI or SNMP of a seed device results in an automatic update of dependent devices in the

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

network. A new device added to the network can receive the configuration automatically, reducing the configuration overhead even further.

Figure 1 illustrates the generic concept. Initial manually configured information will be automatically propagated throughout the network.

Figure 1.

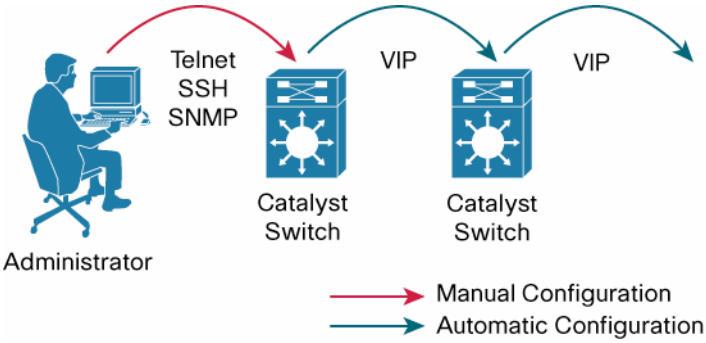
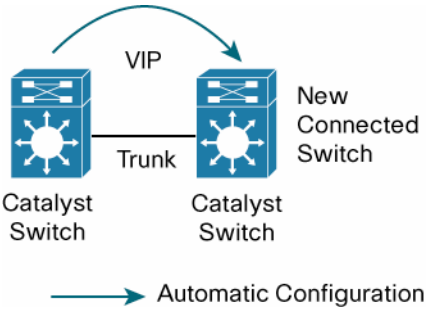


Figure 2 shows automatic provisioning when a new switch is added to a configured network.

Figure 2.



Improved availability and reduced deployment time

Using an configuration tool reduces deployment time. Transferring an approved template throughout the network reliably and automatically ensures stability and improves availability.

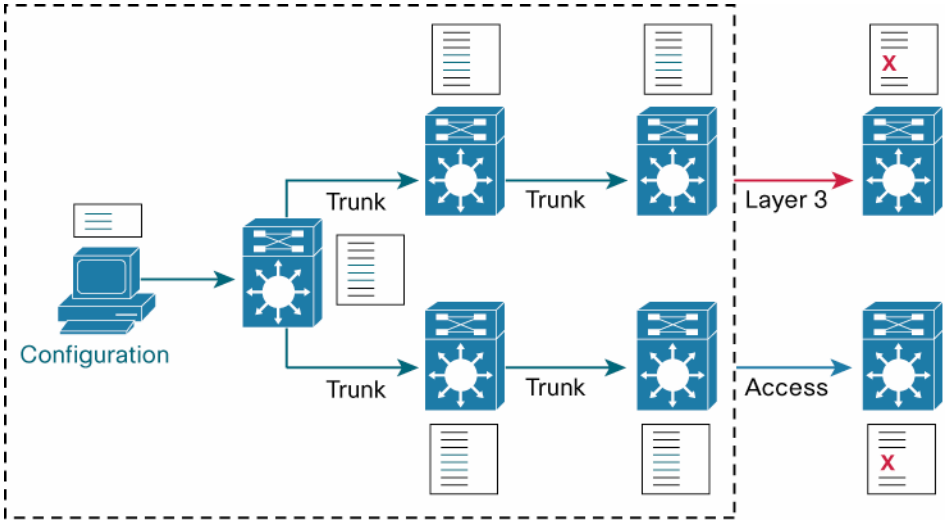
VTP Domain

The size of the VTP distribution area for this automatic configuration is limited by the path of contiguous ISL or Dot1Q trunk sections. A VTP update message can be sent over trunks but not over access ports or Layer 3 interfaces.

Figure 3 illustrates the flow of VTP configuration information via trunk links. This set of configuration statements is indicated by the green lines. The red “X” indicates that a certain configuration set is not available for this device.

Figure 3.

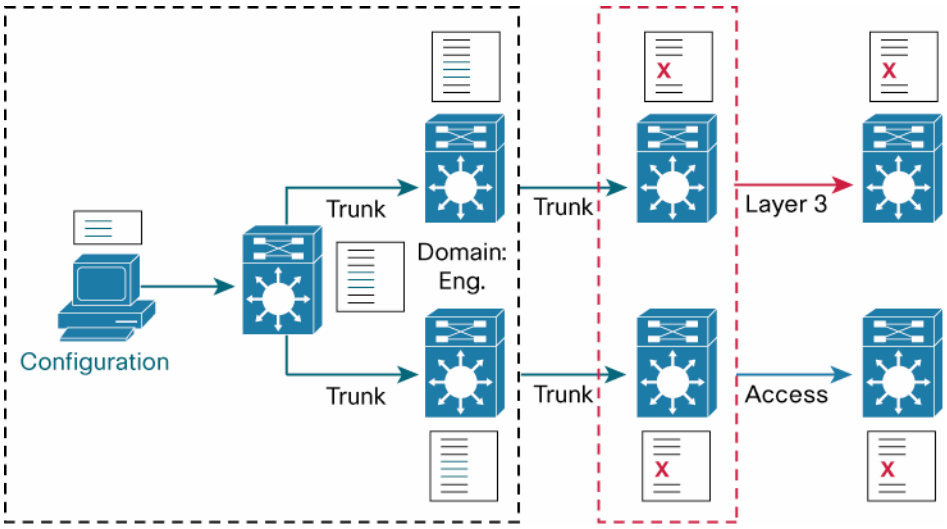
© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.



To define or limit the update area, VTP version 3 uses the same concept of domains as implemented in VTP version 1 and VTP version 2. Only devices belonging to the same VTP domain are able to exchange and process VTP information.

Figure 4 illustrates the case of three devices that are configured with the same domain name of “Eng” and are able to exchange and process VTP update. Devices with the domain name “Sales” will compare the received message with the locally configured domain name. Because the receiving name does not match the configured name the receiving VTP message is ignored and dropped.

Figure 4.



The domain name is manually specified as a text string with a default value of NULL. In previous versions a new switch with the default domain name of NULL used the first received VTP message with a configured domain name and changed itself to this message accordingly. This behavior has changed with VTP version 3, which now requires manual configuration prior to enabling VTP version 3.

Before enabling VTP version 3 one should verify if the VTP domain name is set to a nondefault value and if not done already enabled the use of spanning-tree extended system-id for spanning

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

tree. An explanation of spanning tree is outside the scope of this paper, but the extended system ID allows the switch to support up to 4k individual STP processes, each with a unique ID.

```
Catalyst6500-1(config)#vtp version 3
Cannot set the version to 3 because domain name is not configured.
```

```
Catalyst6500-1(config)#vtp domain 7817
Changing VTP domain name from NULL to 7817
*Jul 8 11:18:33.215: %SW_VLAN-SP-6-VTP_DOMAIN_NAME_CHG: VTP domain name changed to 7817.
```

```
Catalyst6500-1(config)#vtp version 3
Cannot set the version to 3 because spanning-tree extend system-id is disabled.
```

```
Catalyst6500-1(config)#spanning-tree extend system-id
*Jul 8 11:24:23.719: %SPANTREE-5-EXTENDED_SYSID: Extended SysId enabled for type vlan. The Bridge IDs of all active STP instances have been updated, which might change the spanning tree topology.
```

```
Catalyst6500-1(config)#vtp version 3
*Jul 8 11:25:23.203: %SW_VLAN-SP-6-OLD_CONFIG_FILE_READ: Old version 2 VLAN configuration file detected and read OK. Version 3 files will be written in the future.
```

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

```
Catalyst6500-1#show vtp status
VTP Version capable : 1 to 3
VTP version running : 3
VTP Domain Name : 7817
VTP Pruning Mode : Disabled
VTP Traps Generation : Disabled
Device ID : 00d0.bcd2.0c00
Feature VLAN:
--------------
VTP Operating Mode : Server
Number of existing VLANs : 5
Number of existing extended VLANs : 0
Configuration Revision : 0
Primary ID : 0000.0000.0000
Primary Description :
MD5 digest : 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
Feature MST:
--------------
VTP Operating Mode : Transparent
Feature UNKNOWN:
--------------
VTP Operating Mode : Transparent
```

Brief Background on VTP Version 1 and VTP Version 2

VTP version 1 was developed when only 1k VLANs where available for configuration. A tight internal coupling of the VLAN implementation, the VLAN pruning feature, and the VTP function itself offered an efficient means of implementation. It has proved in the field to reliably support Ethernet, Token Ring, and FDDI networks via VTP.

The use of consistent VLAN naming was a requirement for successful use of VMPS (Vlan Membership Policy Server). VTP ensures the consistency of VLAN names across the VTP domain. Most VMPS implementations are likely to be migrated to a newer, more flexible and feature-rich method.

To add support for Token Ring, VTP version 1 was enhanced and called VTP version 2. Certain other minor changes and enhancements were also added at this time.

The functional base in VTP version 3 is left unchanged from VTP version 2, so backward compatibility is built in. It is possible, on a per link basis, to automatically discover and support VTP version 2 devices.

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

VTP version 3 adds a number of enhancements to VTP version 1 and VTP version 2:

- Support for a structured and secure VLAN environment (Private VLAN, or PVLAN)
- Support for up to 4k VLANs
- Feature enhancement beyond support for a single database or VTP instance
- Protection from unintended database overrides during insertion of new switches
- Option of clear text or hidden password protection
- Configuration option on a per port base instead of only a global scheme
- Optimized resource handling and more efficient transfer of information

These new requirements made a new code foundation necessary. The design goal was to make VTP version 3 a versatile vehicle. This was not only for the task of transferring a VLAN DB but also for transferring other databases—for example, the MST database.

If you are interested in more information on earlier VTP versions, please refer to the Appendix.

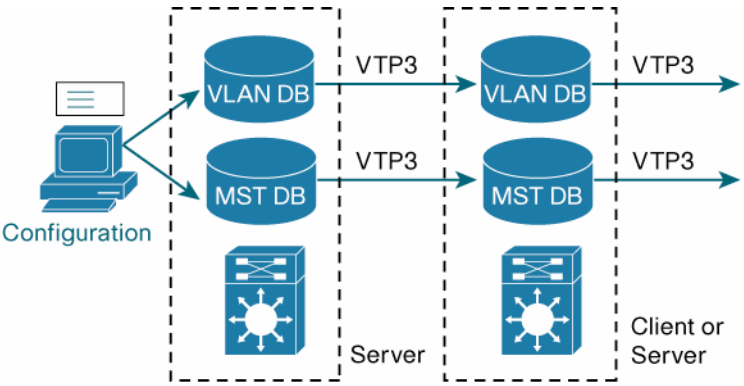
VTP Version 3

VTP version 3 introduces the concept of transferring an opaque database in situations where VTP version 1 and VTP version 2 interacted with the VLAN process directly. By offering a reliable and efficient transport mechanism for a database, usability can be expanded from just serving the VLAN environment. As a first step, VTP version 3 includes support for the MST mapping table.

The transport function for a particular database (or table) is independent from the other and is called a VTP instance.

Figure 5 shows VTP version 3 support for a VLAN instance and a separate MST instance.

Figure 5.



Different kinds of *instances* are mentioned in this paper:

VTP instance: Either the *VLAN database*, the *MST database*, or the *unknown database* instance. This is also called the *VTP Mode*.

MST instance: Support for between 1 and 64 instances or mappings between VLANs and STP calculations: 1 MST STP calculation equals 1 instance.

The *unknown DB* instance serves as a placeholder for forthcoming new features.

Configuration Revision Number

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

The concept of using and comparing the configuration revision number is still used in VPT version 3. Each change of the configuration for an instance automatically increments the configuration revision number. The configuration revision number represents the timeliness and is included in the VTP messages. A device receiving a VTP message compares its own number with the receive one. If the received number is larger than the current number, the local device requests the remote database. The local database will be replaced by the remote database. With VTP version 3, only a specific device in a domain, a primary server, is allowed to update other devices. This new feature reduces the risk of unintended automatic configuration changes, for example, by adding a configured switch with a high configuration revision number to an existing network. The concept of a primary server is discussed in the VTP version 3 operation section.

```
Feature VLAN:
--------------
VTP Operating Mode : Primary Server
Number of existing VLANs : 5
Number of existing extended VLANs : 0
Configuration Revision : 1
Primary ID : 00d0.bcd2.0c00
Primary Description : Catalyst-6500-2
MD5 digest : 0x4F 0x9D 0x78 0xE6 0x53 0x8F 0xED 0x0D
 0x2D 0x66 0x27 0x12 0xF3 0x71 0xAE 0x9B
```

After adding 10 new VLANs (VLAN 401 to 405 and VLAN 4001 to 4005), the configuration revision number increased to 6:

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

```
VLAN Name Status Ports
---- -------------------------------- --------- -----
1 default active
401 VLAN0401 active
402 VLAN0402 active
403 VLAN0403 active
404 VLAN0404 active
405 VLAN0405 active
1002 fddi-default act/unsup
1003 trcrf-default act/unsup
1004 fddinet-default act/unsup
1005 trbrf-default act/unsup
4001 VLAN4001 active
4002 VLAN4002 active
4003 VLAN4003 active
4004 VLAN4004 active
4005 VLAN4005 active
```

```
Feature VLAN:
--------------
VTP Operating Mode : Primary Server
Number of existing VLANs : 10
Number of existing extended VLANs : 5
Configuration Revision : 11
Primary ID : 00d0.bcd2.0c00
Primary Description : Catalyst6500-2
MD5 digest : 0xF9 0xD5 0x35 0x3F 0x0C 0xDF 0x67 0x06
 0x4F 0xF5 0x93 0xB5 0x2B 0x02 0x6C 0x59
```

The configuration revision number works the same in VTP version 3 as in VTP version 1 and VTP version 2 and includes support for VLANs in the extended range region.

VTP Version 3 and CAT OS

VTP version 3 was introduced with CAT OS 8.1(1), and its functionality included the transfer of the VLAN database. To support future features an unknown database instance was prepared. Support for 4k VLANs as well as for Private VLANs was added at that time (CCO JUL-03). Support for a second database, the MST mapping table, was added with CAT OS 8.3(1) and provision for an unknown database was retained for future use.

Because CAT OS is near end of sale (at the time of writing), IOS and modular IOS in Catalyst 6500 will offer the same features with 12.2(33)SXI.

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

The addition of VTP version 3 and interaction between CAT OS and IOS devices creates a soft migration path. Both implementations are able to interact without loss of information or functionality. Transition to IOS and, in particular, modular IOS is now feasible.

The following is a list of CAT OS configuration lines that have to be translated into IOS. The list is not meant to be complete but has been added for convenience and as a start:

Catalyst> (enable) set vtp domain <domain-name> Catalyst6500 (config)# vtp domain <domain-name>
Catalyst> (enable) set spantree macreduction enable Catalyst6500 (config)# spanning-tree extended system-id
Catalyst> (enable) set vtp version [1|2|3] Catalyst6500 (config)# vtp version [1|2|3]
Catalyst> (enable) set vtp mode [vlan|mst|unknown] Catalyst6500 (config)# vtp mode <client|off|server|transparent> <vlan|mst|unknown>
Catalyst> (enable) set vtp mod/port [enable|disable] Catalyst6500 (config-if)# no vtp
Catalyst> (enable) set vtp primary [vlan|mst] {force} Catalyst6500 (config)# vtp primary-server [mst|vlan] {force}
Catalyst> (enable) set vtp password CSSTG {hidden|secret} Catalyst6500 (config)# vtp password <ascii-stirng> {hidden|secret}

MST

For MST the commit task of a configuration for a new instance to VLAN mapping will be available only on a device owning the primary server role for the MST mode (or instance). The commit command is specific to Cat OS and will not be available in IOS. An example is given below.

```
Catalyst> (enable) set spanntree mst 1 vlan 101, 101
Catalyst> (enable) set spanntree mst 2 vlan 102, 202
Catalyst> (enable) set spanntree mst config commit
```

In case the device does not own the primary server role the following message will be displayed:

“MST configuration cannot be changed on a nonprimary server”

For a complete discussion of VTP version 3 with CAT OS, please consult the configuration guides on CCO. For example, the section on CAT OS 8.7 VTP is available at the following link:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/catos/8.x/configuration/guide/vtp.html - wp1017196

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

VTP Version 3 with Native IOS (feature set and version)

With 12.2(33)SXI VTP version 3 will be supported by IOS, closing the feature gap in this area compared to CAT OS. VTP version 3 will be available within all IOS feature sets.

VTP Version 3 Operation

Like VTP version 1 and VTP version 2, VTP version 3 uses the concept of device roles. In addition to the three well-known roles in IOS, *client*, *server*, and *transparent*, a fourth role called *off* is now available. This role is, however, no longer tied to the physical device but to the instance or mode for VTP version 3 operations. The instance can be VLAN or MST

- **Transparent:** A device using a local permanent storage space (for example, NVAM) to hold the locally created configuration of an instance (for example, the VLAN DB). VTP messages are neither sent nor evaluated when received. The local configuration revision number is equal to 0 at all times. Received VTP messages are relayed out of a non-receiving trunk interface if the STP state for VLAN 1 equals forwarding. A domain check, as in VTP version 1, is not implemented.
- **Client:** A device using a local temporary storage space (for example, DRAM) to hold via VTP received information for runtime use. This information is used to update other devices, such as a device that is working as a server. Local configuration of devices in the client role is not possible. After booting, a client device issues a VTP message asking for the configuration of other VTP devices.

  In the case of MST, the default MST configuration will be used at boot time until a VTP version 3 message arrives. Until then, all VLANs are assigned to the default IST instance.
- **Off:** Introduced with CAT OS 7.X, a mode similar to transparent was offered. The difference between transparent and off is the termination of received VTP messages instead of relaying them. With VTP version 3, off mode can be configured globally or on a per port (for example trunk) base. The off mode was formerly only available with CAT OS. The configuration of off on an interface will apply to all VTP instances.

  Turning VTP to off allows a VTP domain to connect to devices in a different administrative domain. Such devices can be switches or servers at a customer or partner site.

  In a global configuration, the off keyword applies to the specified or default instance.

  The third VTP instance (the *unknown* instance) supports only the transparent or off roles.
- **Server:** VTP3 expands and enhances the concept of the server role. The default server role will be the secondary server subtype.

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

```
Catalyst6500-1#show vtp status
VTP Version capable : 1 to 3
VTP version running : 1
VTP Domain Name : 7817
VTP Pruning Mode : Disabled
VTP Traps Generation : Disabled
Device ID : 0012.da44.f800
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 127.0.0.61 on interface EO0/0 (first interface
found)

Feature VLAN:
--------------
VTP Operating Mode : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs : 5
Configuration Revision : 0
MD5 digest : 0x62 0x80 0xF3 0x25 0x0C 0x2E 0xB6 0x06
 0x53 0x15 0x4B 0x3D 0xBF 0xE3 0x0C 0xA5
```

In addition, only one server per domain can be prompted to be a primary server.

client and secondary server devices receive a configuration from a primary server. A secondary server stores the received configuration in a local permanent storage space (for example, NVRAM) and updates other devices in the same domain and for the same instance. In the case of VTP version 1 or VTP version 2, a server can be manually configured via command-line interface (CLI) or Simple Network Management Protocol (SNMP). In VTP version 3, a secondary server cannot be configured manually but can receive updates, similar to a device owning the client role.

One server can be promoted to be a primary server for an instance. There are two instances available at the time of writing: the VLAN instance and the MST instance. Configuration changes can be made only at the primary server itself via either CLI (Telnet or Secure Shell Protocol) or SNMP. The role of a primary server for the VLAN database and the MST database can be divided among two different physical machines or handled by one machine alone.

When a server is designated as the primary server, a sanity check is performed in the domain in advance. The goal is to find conflicting devices by listening for a primary server other than the one configured. A warning message is generated if conflicting devices are discovered. Proceeding with the designation of the primary server overwrites the configuration of all devices in the domain, including any conflicting devices. A configuration option in the form of the force keyword skips the sanity check.

The following sample output illustrates the process of promoting a secondary server to become the primary server.

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

```
Catalyst6500-1#vtp primary vlan
This system is becoming primary server for feature vlan
No conflicting VTP3 devices found.
Do you want to continue? [confirm]
*Jul 8 12:34:20.047: %SW_VLAN-SP-4-VTP_PRIMARY_SERVER_CHG:
00d0.bcd2.0c00 has become the primary server for the VLAN VTP feature.
```

```
Catalyst6500-1#vtp primary mst
This system is becoming primary server for feature mst
No conflicting VTP3 devices found.
Do you want to continue? [confirm]
*Jul 8 12:36:39.553: %SW_VLAN-SP-4-VTP_PRIMARY_SERVER_CHG:
00d0.bcd2.0c00 has become the primary server for the MST VTP feature
```

The default role for the VLAN instance will be server (secondary); for all other instances the default role will be transparent.

```
Feature VLAN:
--------------
VTP Operating Mode : Server
<SNIP>
Feature MST:
--------------
VTP Operating Mode : Transparent
Feature UNKNOWN:
--------------
VTP Operating Mode : Transparent
```

If a secondary server is promoted to become a primary server without specification of the instance (VLAN or MST), the VLAN instance will be specified.

Message Protection and Security

With former VTP implementations an optional md5 digest is available to prevent the alteration of messages in the path from one switch to another. This feature prevents the insertion of new unauthorized switches by keeping the digest secret. The compromise of the digest (or password) due to a simple **show** command, **show vtp** password, (depending on the service-encryption option) or by looking at the vlan.dat file forced a digest change for the entire domain. With VTP version 3 the password can be configured with two options: hidden and secret. When the hidden option is used, the password is not stored in a readable format. A show command or inspection of the vlan.dat file can no longer be used to compromise the password.

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

```
Catalyst6500-1(config)#vtp password Andreas
Setting device VTP password to Andreas
```

```
Catalyst6500-1#show vtp pass
VTP Password: Andreas
```

The content of the file vlan.dat reveals the password in clear text:

```
00000030: 00000000 00000001 30383037 30383133 .... .... 0807 0813
00000040: 32343439 6280F325 0C2EB606 53154B3D 2449 b.s% ..6. S.K=
00000050: BFE30CA5 07416E64 72656173 00C795CE ?c.% .And reas .G.N
00000060: B21E305F 10000000 00000000 00000000 2.0_ .... .... ....
00000070: 00000000 00000000 00000000 00000000 .... .... .... ....
```

Service of password encryption can be added:

```
Catalyst6500-1(config)#service password-encryption
```

The show command stops displaying the clear text password, but the vlan.dat file still contains the password in a readable format.

```
Catalyst6500-1#show vtp password
VTP Encrypted Password: 02270A5F19030E32
```

To protect the password the new hidden option should be used:

```
Catalyst6500-1(config)#vtp password Cisco hidden
Setting device VTP password
```

```
Catalyst6500-1#show vtp password
VTP Password: CF94C2FF1CDCEB8DC795CEB21E305F10
```

The vlan.dat file no longer contains a readable password:

```
00000030: 00000000 00000001 30383037 30383133 .... .... 0807 0813
00000040: 34323334 6280F325 0C2EB606 53154B3D 4234 b.s% ..6. S.K=
00000050: BFE30CA5 00CF94C2 FF1CDCEB 8DC795CE ?c.% .O.B ..\k .G.N
00000060: B21E305F 10000000 00000000 00000000 2.0_ .... .... ....
```

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

To apply a password in the secure form to a configuration, the second option “secret” has to be specified.

When changing the device role from secondary server to primary server the password will be requested if the hidden option was specified in advance.

Operation for VLANs

Any change in the characteristic of the VLAN database will increment the configuration revision number and trigger a VTP version 3 message. A change of characteristic can be one or all of the following (not a complete list):

- Addition (for example, creation) or removal (for example, deletion) of a VLAN
- State change of a VLAN (active or suspended)
- Change of VLAN name or MTU

Assuming a stable configuration every 300 seconds, a VTP version 3 message (Summary Advert) is issued to synchronize all devices in the domain. This update mechanism has not changed from VTP version 1 or VTP version 2. A significant enhancement in VTP version 3 is the ability to support more than the legacy 1k VLANs; VLANs up to 4k are now supported.

Depending on the chassis in use, this command might be present by default. All chassis equipped with 64 MAC addresses instead of the 1k version will have the extended system-id command enabled as a default. The reduced MAC address pool can be found in all Cisco E-Series chassis and the Cisco Catalyst 6513.

In addition, the formerly reserved VLAN range of 1002 to 1005 might be available for use in an Ethernet environment in the future. At the time of writing, the four VLANs are still unsupported and not usable.

Those VLANs were formerly used for FDDI and Token Ring:

```
VLAN Name Status Ports
---- -------------------------------- --------- -------------
1 default active Fa1/24, Gi5/2
1002 fddi-default act/unsup
1003 trcrf-default act/unsup
1004 fddinet-default act/unsup
1005 trbrf-default act/unsup
```

Since Catalyst 6000/6500 Series switches no longer support FDDI or Token Ring (unlike the Catalyst 5000/5500 Series), those VLANs might be usable in an Ethernet-only environment in the future.

The change of the media type to Ethernet is currently not supported.

```
Catalyst6500-1(config-vlan)#media ethernet
Default VLAN 1005 may not have its type changed.
```

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

The VLAN range from 1006 up to 1023 is still reserved for internal functions like GOLD and specific processes (housekeeping functions).

```
1006 online diag vlan0
1007 online diag vlan1
1008 online diag vlan2
1009 online diag vlan3
1010 online diag vlan4
1011 online diag vlan5
1012 PM vlan process (trunk tagging)
1013 Control Plane Protection
1014 L3 multicast partial shortcuts for VPN 0
1015 Egress internal vlan
1016 Multicast VPN 0 QOS vlan
1017 IPv6 Multicast Egress multicast
```

Hidden VLANs

A VLAN is used for a couple of internal features, including support of Layer 3 interfaces. In the following example, the interface Fast Ethernet 1/24 is used in routed mode:

```
Catalyst6500-1#show run int fast 1/24
Building configuration...

Current configuration : 69 bytes
!
interface FastEthernet1/24
 ip address 10.0.1.1 255.255.255.0
end
```

The VLAN 1018 is automatically allocated for this interface.

```
Catalyst6500-1#show vlan internal usage

VLAN Usage
---- --------------------
<SNIP>
1018 FastEthernet1/24
```

Creating the VLAN 1018 on the remote primary server works as expected:

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

```
VLAN Name Status Ports

---- -------------------------------- --------- ---------------------

<SNIP>

1018 VLAN1018 active

<SNIP>
```

Because this VLAN 1018 is allocated as an internal VLAN, it will not be available on C6o.

Plan VLAN numbering in advance and adjust the internal VLAN allocation policy accordingly. With the default allocation policy the switch starts to allocate beginning at 1018. The author recommends changing the internal VLAN allocation to start with 4094 and the administrative (CLI/SNMP) allocation to start with 1018.

After shutting down the interface Fast Ethernet 1/24, the internal VLAN number 1018 would be available. After 5 minutes the primary server sends out a summary advertisement that retains the revision number of 12. VLAN 1018 will not be added to the switch.

```
*Jul 13 09:02:09.831: SP: VTP LOG RUNTIME: VTP3[VLAN]: received summary
advertisement packet


*Jul 13 09:02:09.831: SP: VTP LOG RUNTIME: VTP3: dropping the packet 1


*Jul 13 09:04:35.585: SP: VTP LOG RUNTIME: VTP3[VLAN]: tx vtp summary,
domain 78

18, rev 12 window 100
```

```
Feature VLAN:

--------------

VTP Operating Mode : Server

Number of existing VLANs : 10

Number of existing extended VLANs : 5

Configuration Revision : 12

Primary ID : 00d0.bcd2.0c00

Primary Description : c6u

MD5 digest : 0x7C 0xA5 0xC3 0x86 0x88 0x41 0x71 0x61

 0xAC 0xDD 0x72 0xA7 0x8A 0xA6 0x5C 0xE4
```

Changing the characteristic of VLAN 1018 on the initiating device by modifying the name results in an increment of the configuration revision number from 12 to 13 and an update of all devices.

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

```
Catalyst6500-2(config)#vlan 1018
Catalyst6500-2(config-vlan)#name ALQ1018
Catalyst6500-2(config-vlan)#end
```

```
Catalyst6500-2#show vlan
<SNIP>
1018 ALQ1018 active
<SNIP>
```

```
Feature VLAN:
--------------
VTP Operating Mode : Server
Number of existing VLANs : 10
Number of existing extended VLANs : 6
Configuration Revision : 13
Primary ID : 00d0.bcd2.0c00
Primary Description : c6u
MD5 digest : 0x3F 0x5B 0x2B 0x06 0x2F 0x3E 0x3D 0x7E
 0x1F 0xD4 0x08 0x12 0x9D 0x57 0x69 0x4D
```

Enabling the interface FastEthernet 1/24 allocates the next free VLAN in this test environment, 1019:

```
1019 FastEthernet1/24
```

PVLAN

In environments such as those inside the DMZ or with server hosting, a logical separation inside the Layer 2 domain (that is, inside the VLAN) is needed. In this instance, devices are configured using a general IP address pool, but Layer 2 communication between these devices is general not allowed. There are a few exceptions, including server clusters, where inter node Layer 2 communication is required. But those groups are not allowed to communicate on Layer 2 with other clusters or with isolated hosts. The Private VLAN structure is available to accommodate those requirements; the primary VLAN and all dependent secondary VLAN modes are supported by VTP version 3:

- Private VLAN type **Primary**
- Private VLAN type **Secondary Isolated**
- Private VLAN type **Secondary Community**
- Private VLAN type **Secondary 2Way Community**

A downsized version of PVLAN, PVLAN edge, allows local configuration of the PVLAN structure and is implemented in fixed switches like the Cisco Catalyst 3560/3750. The PVLAN feature as

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

implemented in Catalyst 6500 switches allows interaction for a group of switches. The primary VLAN as well as the secondary VLANs are allowed to exist on multiple devices connected by trunks. Members of a community VLAN are supported on one or multiple devices. Use of VTP version 3 to propagate PVLAN information, especially in security-sensitive environments like the DMZ, reduces the risk of incorrect or partly incorrect configurations due to human error.

RSPAN Support

An RSPAN VLAN offers a unique method of transferring monitored SPAN traffic from one device over trunk links to another device. Transfer of data is achieved using a specific VLAN, which is referred to as an RSPAN VLAN. Any device that supports RSPAN should disable Content Addressable Memory (CAM) learning for such VLANs. VTP uses a specific TLV to signal whether a VLAN is an RSPAN VLAN. RSPAN support is included in VTP version 3.

VLAN Pruning

A pruning mechanism has been implemented into VLAN Trunk Protocol (VTP) to optimize the available bandwidth on trunks. As with both earlier VTP versions, pruning is available with VTP version 3 for the first 1k VLANs except VLAN1.

```
Catalyst6500-1#vtp pruning
Pruning switched on
```

Pruning affects only multicast and unknown unicast traffic; multicast traffic is not limited. This is important because VTP pruning will not affect the STP process. In particular, the STP domain (hop count) is not altered nor is the number of logical ports optimized. Manual pruning of VLANs inside trunk links is recommended to influence the STP environment.

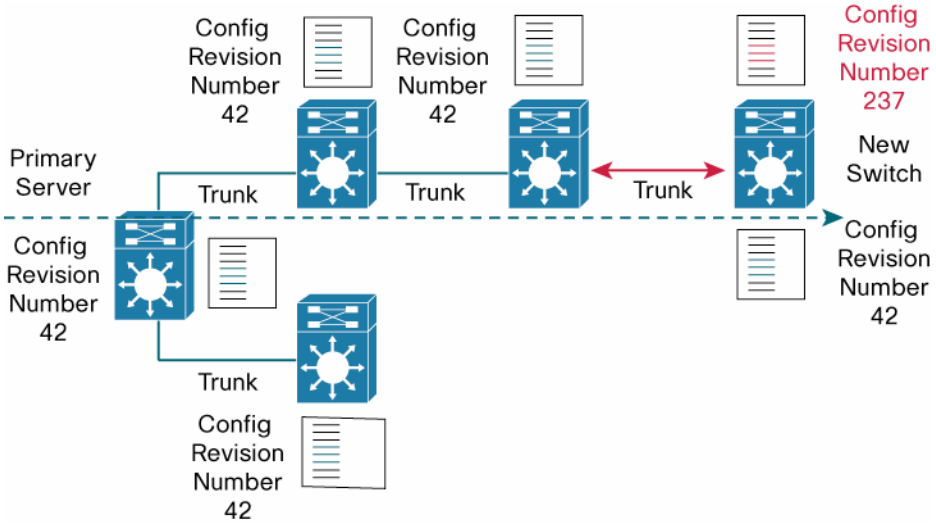
Adding Switches to a Domain

Adding a configured switch to a VTP version 1 or VTP version 2 domain imposed a risk of updating the domain with invalid information that might still be stored in the newly connected switch. In this instance, the VLAN database could be overwritten in a VTP version 1 or VTP version 2 domain based on the configuration revision number. Any client or server device has been able to overwrite the entire domains configuration. In VTP version 1 and VTP version 2, only the configuration revision number was compared, and no further sanity check was available. With VTP version 3 the addition of a configured switch imposes no threat from an unintended update, since only a switch in VTP primary server mode is able to update the domain. A newly introduced server in secondary server mode will therefore never update the domain unintentionally. A former primary server that is reconnected to a domain after a reload will revert automatically to secondary server mode.

Figure 6 illustrates a new switch (upper right) being connected to an existing network. The new switch holds its own configuration and a configuration revision number of 237. Even though 237 is higher than 42, the new switch is not able to update the domain, as would happen with VTP version 1 or VTP version 2. In VTP version 3 only the primary server is able to update the domain and the new secondary server. The new switch will receive the configuration from the network and adjust its configuration revision number to 42.

Figure 6.

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.



Operation with MST

Several spanning tree implementations are available with Cisco Catalyst switches and with the Catalyst 6500 Series in particular. One of them should be chosen based on the individual requirements of the network where it will be implemented. The default Spanning Tree Protocol with CAT OS changed from PVST or PVST+ to Rapid-PVST. With IOS, however, the default STP is still PVST or PVST+. For a complete discussion of STP, please see the documentation and configuration manuals on Cisco Connection Online. To accommodate the requirements of metro area and the data center environments, MST or IEEE 802.1s is often the appropriate choice and offers among other features the following benefits:

- **Fast convergence** due to rapid spanning tree behavior inside the MST domain
- **Increased maximum hop count** (20 default or up to 40, instead of 7 as with IEEE802.1D)
- **Use of the long cost mode** (IEEE 802.1t) to differentiate between GE, GEC, 10GE, and 10GEC without manual and error-prone configuration

In both environments (metro and data center), a high number of switches are typically used. An automatic provisioning function like VTP serves perfectly in these environments.

To use MST, a user has to set up each switch with a general configuration. This configuration includes two separate text strings (domain name and revision number) that when combined represent the domain. A switch determines this configuration by comparing messages against the configured domain, checking if a neighboring switch belongs to a domain or not. As a reminder, you will benefit from MST only if the switches running MST are in the same domain. Otherwise, two switches will be connected via a boundary link, and timer-based convergence occurs as well as a termination of all MST instances besides CST/IST. The mapping table is a second set of information that must match between the two switches. This mapping table consists of the MST instance and the assigned VLAN or group of VLANs. A pre-standard implementation allowed up to 16 instances compared with the 64 instances of the final standard.

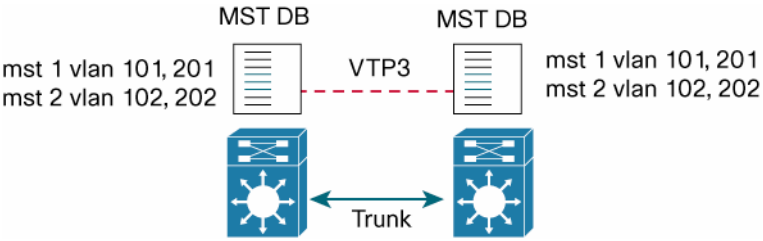
This mapping table can be exchanged using VTP version 3. Two TLVs are used to transfer the MST table. One TLV stores the configuration name and revision number. This allows receiving devices to determine if the information corresponds to the local configuration. The second TLV carries the VLAN or VLAN group mapping to an MST instance. Only those MST instances that are

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

used will be transmitted, thereby optimizing resources to build the updates and bandwidth on the path.

Figure 7 illustrates the transfer of two MST instances 1 and 2 and the corresponding VLANs.

Figure 7.



Using MST along with VTP version 3 for configuration makes all MST inherited benefits available and limits the increase in configuration overhead.

Use of VTP version 3 further reduces the risk of non-homogeneous configuration regardless of the number of switches and repetitive configurations.

Table 1. VTP Roles Versus Functions and Behavior

MST – VTP3	Relay/Process	Configure	Save
PRIMARY SRV	Yes	Yes	Yes
SECONDARY SRV	Yes	**No**	Yes
CLIENT	Yes	**No**	**No**
TRANSPARENT	Yes	Yes	Yes
OFF	**No**	Yes	Yes

To use VTP version 3 for MST the role has to be changed from transparent to server. Promotion of the device where the configuration will be changed to become a primary server is necessary:

```
Feature MST:
--------------
VTP Operating Mode : Primary Server
Configuration Revision : 2
Primary ID : 00d0.bcd2.0c00
Primary Description : c6u
MD5 digest : 0xFF 0x60 0xBA 0x93 0x2D 0xA5 0xEA 0x09
 0x06 0x8D 0xC7 0x6C 0xD1 0xD9 0x4D 0xD7
```

Three MST instances will be created on the primary server:

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

```
Catalyst6500-2#show spanning-tree mst configuration
Name [MST]
Revision 1 Instances configured 3
Instance Vlans mapped
-------- ---------------------------------------------------------------
0 2-400,406-4000,4006-4094
1 1,401-405
2 4001-4005
-------------------------------------------------------------------------
```

Even without changing the spanning-tree mode from PVSTP to MST, the MST configuration is received and available:

```
Catalyst6500-1#show spanning-tree mst configuration
% Switch is not in mst mode
Name [MST]
Revision 1 Instances configured 3

Instance Vlans mapped
-------- ---------------------------------------------------------------
0 2-400,406-4000,4006-4094
1 1,401-405
2 4001-4005
-------------------------------------------------------------------------
```

And after enabling MST:

```
Catalyst6500-1#show spanning-tree mst configuration
Name [MST]
Revision 1 Instances configured 3

Instance Vlans mapped
-------- ---------------------------------------------------------------
0 2-400,406-4000,4006-4094
1 1,401-405
2 4001-4005
-------------------------------------------------------------------------
```

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Configuration changes are only available at the device that is the primary server for the MST instance. If not, a warning message is displayed after you leave the MST configuration section:

```
Catalyst6500-1(config)#spanning-tree mst configuration
Catalyst6500-1(config-mst)#instance 4 vlan 1018
Catalyst6500-1(config-mst)#end
MST region is not configurable as the system is not the primary server for MST database
```

Adding the new VLAN instance 4 on the primary server updates the entire VTP domain:

```
Catalyst6500-1#show spanning-tree mst con
Name [MST]
Revision 1 Instances configured 4

Instance Vlans mapped
-------- ---------------------------------------------------------------
0 2-400,406-1017,1019-4000,4006-4094
1 1,401-405
2 4001-4005
4 1018
-------------------------------------------------------------------------
```

Interoperability

VTP3 interoperates with VTP version 2 but not VTP version 1. For devices that are capable of running VTP version 2 but are running in VTP version 1 mode, a change to VTP version 2 is triggered by the VTP version 3 device. Before considering VTP version 3 for your network it is recommended that you verify if all switches in the existing or prospective VTP domain are capable of running in VTP version 2 mode. The best results will be achieved in a homogeneous VTP version 3 environment.

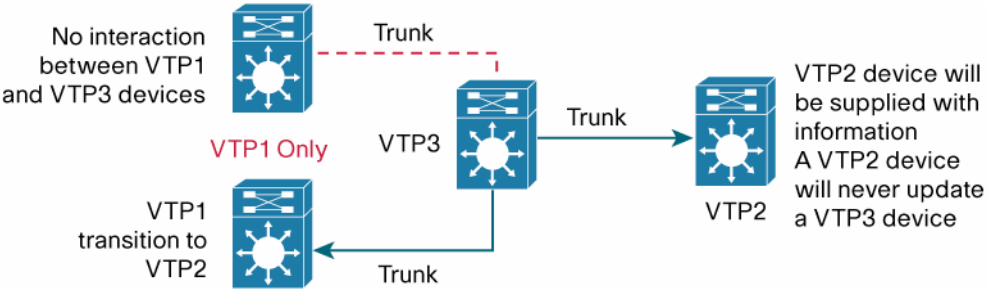
Interoperability with VTP Version 1 and VTP Version 2

After receiving VTP version 2 advertisements, a VTP version 3 device sends, on a per port basis, in addition to VTP version 3 messages, a VTP version 2–compatible database or message out of that receiving link. This behavior will continue as long a VTP version 2 messages are being received. There is no interaction available for VTP version 1-only devices. The recommendation is to use VTP version 3 throughout the domain.

Figure 8 illustrates the interaction possibilities between VTP version /VTP version 2 and VTP version 3 devices.

Figure 8.

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.



When using server mode for MST, a switch back to VTP version 2 is not possible.

```
Catalyst6500-1#vtp version 2
MST Server mode is not supported in version 2. Configure the MST VTP
mode to Transparent before changing the version to 2.
```

Best Practices and Tips

All resources on a switch are limited. This holds true for storage space and therefore the space used for the VLAN database should be limited by using VLAN names with less than 20 characters.

To optimize the convergence time in the event of powering up multiple or all devices (after an outage, etc.) the MST instance should be in VTP version 3 server mode in order to use the last saved configuration rather than kick-start VLAN-to-IST mapping.

To avoid issues when mixing VTP version 3 and VTP version 2, the VTP version 2 mode should be set to client. However, the best results will be achieved within a homogeneous VTP version 3 environment. If feasible, all devices should be upgraded to support VPT version 3.

Risks and Dependencies

The use of VTP version 3 itself imposes no known risk worth mentioning.

A risk of unintended behavior in a mixed environment with VTP version 2 is possible. A careful evaluation of the network design and VTP roles is essential and recommended.

VTP version 3 will be available starting with 12.2(33)SXI. A software upgrade is therefore needed to implement VTP version 3 functionality. Support for individual components of a modular system will vary. Legacy modules must be phased out over time and support for some older line cards is canceled in 12.2(33)SXH or 12.2(33)SXI, for example. The resulting risk of using VTP version 3 is the potential lack of module support.

Summary

VTP version 3 offers a reliable solution in terms of improved administrative control. Support for more VLAN features is provided and usability is significantly expanded. All 4k VLANs are now supported with VTP version 3. DMZ structures benefit from VTP version 3 because of its support for the PVLAN feature. One other notable improvement is the support for additional databases like MST. For service providers and data centers an efficient and reliable provisioning function is now available in IOS.

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

CLI

All the **show** commands should be verified against the latest official command reference guide. The information in the following sections is subject to change.

Configuration

VTP version 3 configuration is mostly performed in global configuration mode. The first block of commands is, however, issued from normal exec mode.

```
Catalyst6500-1#vtp ?
 password Set the password for the VTP administrative domain.
 primary Make the system as the primary server
 pruning Set the administrative domain to permit pruning.
 version Set the administrative domain VTP version
```

```
Catalyst6500-1#vtp password ?
WORD The ASCII password for the VTP administrative domain.
```

```
Catalyst6500-1#vtp primary ?
 force Do not check for conflicting devices
 mst MST feautre
 vlan Vlan feautre
 <cr>
```

```
Catalyst6500-1#vtp version ?
 <1-2> Set the administrative domain VTP version number
```

The following commands are issued from configuration mode:

```
Catalyst6500-1(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
```

```
Catalyst6500-1(config)#vtp domain ?
 WORD The ASCII name for the VTP administrative domain.
```

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

```
Catalyst6500-1(config)#vtp mode ?
 client Set the device to client mode.
 off Set the device to off mode.
 server Set the device to server mode.
 transparent Set the device to transparent mode.
```

```
Catalyst6500-1(config)#vtp mode client ?
 mst Set the mode for MST VTP instance.
 unknown Set the mode for unknown VTP instances.
 vlan Set the mode for VLAN VTP instance.
 <cr>
```

```
Catalyst6500-1(config)#vtp version ?
 <1-3> Set the adminstrative domain VTP version number
```

```
Catalyst6500-1(config)#vtp password Cisco ?
 hidden Set the VTP password hidden option
 secret Specify the VTP password in encrypted form
 <cr>
```

With VTP version 3, configuration on a per interface basis (also known as Interface OFF mode) is available:

```
Catalyst6500-1(config)#interface fast 1/24
Catalyst6500-1(config-if)#no vtp ?
```

Verification and Troubleshooting

The show commands have been enhanced to support VTP version 3. Specifically for VTP version 3 new commands were added:

```
Catalyst6500-1# show vtp status                    enhanced cmd
```

The output will vary depending on the VTP version used. In the following sample output, a device running VTP version 3 is used:

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

```
Catalyst6500-1#show vtp status

VTP Version capable : 1 to 3
VTP version running : 3
VTP Domain Name : 7817
VTP Pruning Mode : Enabled
VTP Traps Generation : Disabled
Device ID : 00d0.bcd2.0c00

Feature VLAN:
--------------
VTP Operating Mode : Server
Number of existing VLANs : 5
Number of existing extended VLANs : 0
Configuration Revision : 0
Primary ID : 0000.0000.0000
Primary Description :
MD5 digest : 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00


Feature MST:
--------------
VTP Operating Mode : Server
Configuration Revision : 0
Primary ID : 0000.0000.0000
Primary Description :
MD5 digest : 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00


Feature UNKNOWN:
--------------
VTP Operating Mode : Transparent
```

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

When using VTP version 3 this command displays information regarding the configured instance or database (VLAN, MST, unknown).

```
Catalyst6500-1 # show vtp devices [conflicts] [feature]
                                                    new cmd
```

This new command actively queries the domain and displays all discovered devices. Only server and client devices will respond and therefore be included in the list. The additional but optional keyword conflict restricts the display to only conflicting devices, which would be overridden if the device where the show command was issued would be promoted to become a primary server.

```
Catalyst6500-1#show vtp devices
Retrieving information from the VTP domain. Waiting for 5 seconds.
No VTP3 devices found.
```

After promoting c6u to become a primary server a neighbor is displayed.

```
Catalyst6500-2#show vtp dev
Retrieving information from the VTP domain. Waiting for 5 seconds.
VTP Feature Conf Revision Primary Server Device ID Device Description
--------- ---- -------------- -------------- -------------- -----------
--
VLAN      No 1 00d0.bcd2.0c00 0012.da44.f800 Catalyst6500-
```

```
Catalyst6500-1#show vtp dev
Retrieving information from the VTP domain. Waiting for 5 seconds.

VTP Feature Conf Revision Primary Server Device ID Device Description
--------- ---- -------- -------------- -------------- -------------
VLAN      No 1 00d0.bcd2.0c00=00d0.bcd2.0c00 Catalyst6500-
```

Some “borrowed” older examples:

```
WBU # show vtp devices
Gathering information from the domain, please wait.
VTP Database Conf switch ID Primary Server Revision System Name
 lict
------------ ---- -------------- ------ ---------- ----------
VLAN         No   000c.0012.3456=000c.0012.3456 1001 WBU
MST          No   000c.0012.3456=000c.0012.3456 42   WBU
```

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

One neighbor with two instances is shown. The neighbor is the primary server for both the VLAN and the MST instance.

```
VLAN Yes 000c.0065.4321 0004.0012.3456 1024 WBU
```

One neighbor that received its VLAN database from 0004.0012.3456 is at a different address than the system where the show command was issued.

```
MST No 00b0.0012.3456 0004.0065.4321 1234 WBU
```

The neighbor 00b0.0012.3456 used the same primary server for the MST mapping table.

A conflict is detected if the discovering and the discovered device received their configuration from different primary servers. A conflict can occur on a per instance basis.

```
Catalyst6500-1 # show vtp counters                    unchanged
```

```
Catalyst6500-1#show vtp counters
VTP statistics:
Summary advertisements received : 0
Subset advertisements received : 0
Request advertisements received : 0
Summary advertisements transmitted : 0
Subset advertisements transmitted : 0
Request advertisements transmitted : 0
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
 non-pruning-capable device
---------------- ---------------- ---------------- --------------------
-------
```

Appendix

History of VLAN Trunking Protocol

VTP

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

The history of VTP goes back to the Cisco Catalyst 5000. The first VTP implementation was available within a Catalyst 2900/5000 running CAT OS v2.1 and ATM v3.1 software. Catalyst 3000 switches had supported VTP since software version 2.0

VTP uses a Layer 2 signaling or messaging protocol using a Cisco multicast address and a specific SNAP Ethernet type code: 01-00-0C-CC-CC-CCC and 0x2003.

VTP uses CDP and PAgP VLAN1 when traversing a trunk link. This holds true even if VLAN 1 for user traffic is pruned.

Signaling is supported only over trunk links. Trunk links can be either dot1q or ISL.

Resources

Understanding VLAN Trunk Protocol (VTP):
http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a0080094c52.shtml

Configuring VTP (CAT OS 8.7):
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/catos/8.x/configuration/guide/vtp.html - wp1017196

Acronyms

GARP	Generic Attribute Registration Protocol
GVRP	GARP VLAN Registration Protocol
GMRP	GARP Multicast Registration Protocol
LAN	Local Area Network
MST	Multiple Spanning Tree
PVLAN	Private VLAN
STP	Spanning Tree Protocol
TLV	Tag Length Value
VLAN	Virtual LAN
VMPS	VLAN Membership Policy Server
VTP	VLAN Trunking Protocol

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)

Printed in USA C78-508010-00 11/08

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.