## OVERVIEW

VTP (VLAN Trunking Protocol)—Isn't a trunking protocol—it simply happens to send its messages over trunks. It is an OSI L2 protocol that allows switches to learn VLANs from each other, simplifying the process of adding a VLAN to all switches in a portion of a network. Which interfaces are in which VLANs remains unique to each switch.

VLAN Ranges—Switches that use VTP are limited to the standard range of VLANs (1-1005). 2-1001 are configurable. 1 is already on every switch as the default VLAN and 1002-1005 are reserved for historical purposes. Switches that are configured with VTP in transparent mode or off can use the extended range through 4094. VLANs 0 and 4095 are reserved.

VTP Modes—As you can see, even though a client cannot create VLANs, a client can advertise any it already has and a server can learn them. Ick.

| | SERVER | CLIENT | TRANSPARENT | OFF |
|---|---|---|---|---|
| Advertises VLANs | • | • | | |
| Learns VLANs | • | • | | |
| Passes Advertisements On | • | • | • | |
| Can Create VLANs 2-1001 | • | | • | • |
| Can Create VLANs 1006-4094 | | | • | • |

The first three modes are set in config; turning VTP completely off requires a recent version of IOS.

```
S2(config)# vtp mode { server | client | transparent }
S2# vtp mode off
```

VTP Domain—Group of switches whose VLAN configs will match thanks to VTP.

Configuration Revision Number—Each time a VLAN within a server's VLAN configuration database is updated, the revision number of the database is incremented. In response, all other switches in the domain will update their VLAN databases and revision numbers to match. This mechanism cleanly handles the situation where you have multiple servers but creates a danger when a new switch of unknown VTP revision number joins the domain, even as a client. Servers will learn VLANs from other servers with a higher revision number, just like clients.

Periodic Updates—Every 5 minutes (default) servers & clients send updates which include the revision number. Any switch (server or client) receiving an update with a higher revision number than its own updates its confg to match

VTP Requirements Between Switches

- Link between switches operating as a trunk (802.1Q vs. ISL doesn't matter)
- VTP Domain name must match (case-sensitive)
- VTP Password must match (case-sensitive; null on all is a match)

VTP Versions 1 and 2 (ignore version 3 for CCNA)—The only thing we care about is that in order for a transparent mode switch to pass advertisements on, its VTP version must match. For clients and servers, you *should* make the versions match, but they'll still exchange VLAN configs if you don't.

## VTP PRUNING

By default, switches flood broadcasts within a VLAN out trunks along with frames to unknown destinations. Because VTP ensures that all switches in a domain have the same VLANs, these broadcasts will propagate throughout the domain, even to switches that have no hosts in that VLAN. Hosts will still be spared broadcasts not in their own VLAN, but the switches and the links between switches won't.

A switch that knows about a VLAN thanks to VTP but has no access ports in that VLAN can request through VTP that its neighbors stop sending frames in that VLAN over the trunk they share.

## CONFIGURATION

All VTP configs are done in global config; there is no sub-mode.

| | S1 | S2 |
|---|---|---|
| 1 | `vtp mode server` | `vtp mode client` |
| 2 | `vtp domain MY_VTP_DOMAIN` | `vtp domain MY_VTP_DOMAIN` |
| 3 | `vtp password myPassword` | `vtp password myPassword` |
| 4 | `vtp pruning` | *Can't set pruning on a client* |
| 5 | `vtp version 1` | `vtp version 1` |

Details:

- VTP mode defaults to server
- The VTP domain defaults to null. When you set the domain name on one server in the null domain, it automatically propagates to all switches in the null domain.
- VTP version defaults to 1 in IOS 12.2
- VTP pruning disabled by default in IOS 12.2
- There is no "secret" version of the vtp password
- VTP pruning can only be set on a server
- Just like VLAN configurations, none of these VTP configs show up in the running-config unless VTP is in transparent mode! VTP servers and clients store their VLANs and VTP configurations in the file vlan.dat instead.

## VERIFICATION

```
S1# show vtp status
VTP Version                     : running VTP1 (VTP2 capable)
Configuration Revision          : 4
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 8
VTP Operating Mode              : Server
VTP Domain Name                 : MY VTP DOMAIN
VTP Pruning Mode                : Enabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xB2 0x7F 0xAC 0x64 0xB3 0xD3 0xC0 0xC8
Configuration last modified by 10.0.0.1 at 3-1-93 02:17:19
Local updater ID is 10.0.0.1 on interface Vl1 (lowest numbered VLAN interface found)
```

*This final line only appears on VTP servers.*

```
S2# show vtp status
VTP Version                     : running VTP1 (VTP2 capable)
Configuration Revision          : 4
```
*This is the configuration revision number of the VLAN database. A higher advertised number will cause all servers and clients in the domain to change their VLANs to match.*
```
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 8
```
*Only three of these are my VLANs. One is VLAN 1, and the others are VLANs 1002-1005.*
```
VTP Operating Mode              : Client
VTP Domain Name                 : MY_VTP_DOMAIN
VTP Pruning Mode                : Enabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xB2 0x7F 0xAC 0x64 0xB3 0xD3 0xC0 0xC8
*** MD5 digest checksum mismatch on trunk: Fa0/23 ***
```
*This warns you that switch S3, located out fa0/23, is using a different VTP password and/or domain name, disabling VTP sharing across that trunk. The digest shown is an MD5 hash of the VTP domain name and VTP password together. If either differs, the hash won't match.*
```
Configuration last modified by 10.0.0.1 at 3-1-93 02:17:19
```
*This IP address is on the switch's SVI (interface vlan 1) and are more helpful that having all switches named "0.0.0.0."*

*The timestamp is completely bogus because I haven't set the clocks on these switches. NTP could be very useful here.*

The VTP password isn't show in the above command and isn't in the running-config (no VTP configs are unless you're in VTP transparent mode), but you can still get it.

```
S2# show vtp password
VTP Password: myPassword
```

## CLEARING A CONFIG

First shutdown your trunks to stop VTP from re-sharing what you're deleting, then delete the vlan.dat file from flash using the "delete" command, not "erase." (memory hint: both vlan.Dat and Delete have Ds in them.)

## TROUBLESHOOTING

Basically, VTP failures boil down to a pair of switches not synchronizing. You'll probably spot the problem because the list of VLANs will be wrong on one switch. When you find a pair that differ, don't worry about which is right, just find why they're not the same.

- Are they connected by a trunk (operational mode) that's working?

```
S1# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
S2               Fas 0/12          177           S I      WS-C3550- Fas 0/12

S1# show interfaces status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/11                       notconnect   1            auto   auto 10/100BaseTX
Fa0/12                       connected    trunk      a-full  a-100 10/100BaseTX
Fa0/13                       notconnect   1            auto   auto 10/100BaseTX
```

```
S1# show interfaces fa0/12 switchport
Name: Fa0/12
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: trunk
```

*Mr. Odom prefers this command. Make sure you include the "switchport" keyword*

- Do the VTP domain name and password match (case sensitive)? Null values are fine as long as they match. If they both match, the MD5 hash will match (it's a combo of the two).

```
S2# show vtp status
```

*For the domain name and the MD5 hash*

```
VTP Version                     : running VTP1 (VTP2 capable)
Configuration Revision          : 4
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 8
VTP Operating Mode              : Client
VTP Domain Name                 : MY_VTP_DOMAIN
VTP Pruning Mode                : Enabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xB2 0x7F 0xAC 0x64 0xB3 0xD3 0xC0 0xC8
*** MD5 digest checksum mismatch on trunk: Fa0/23 ***
```

*This little tidbit tells us that there's a domain name or password mismatch with the switch out fa0/23 (switch 3).*

```
Configuration last modified by 10.0.0.1 at 3-1-93 02:17:19

S1$ show vtp password
```

- If the VTP pruning setting doesn't match you've probably made a mistake, but not one that would interfere with VTP synchronization.

Mismatched settings that DON'T interfere with synchronization:

- VTP Pruning
- VTP Version

Also, VTP only shares information about VLANs themselves, not how they're used, so the following configation differences from one switch to the next don't indicate a synchronization problem

- VLAN shutdown status
- VLAN interface assignments

## NUCLEAR WINTER

This is my name for the long winter a network administrator can spend queuing up at soup kitchens and job fairs after accidentally connecting a switch with a high configuration revision number to the production network. Existing VTP clients *and servers* with a lower configuration revision number will happily change their VLANs to match, even if the new switch is only a client. Any deleted VLANs will leave assigned interfaces behind, rendering those interfaces unusable.

All of this will happen almost instantly. You can't avoid it; your phone is going to ring …unless you had the foresight to install an IP telephony solution from Cisco, in which case your phones will be down too, giving you time to fix the problem in peace while your coworkers search the building for torches and pitchforks, readying their final assault on the datacenter.

The worst part is that defaults help this happen:

- Domain names and passwords default to null and therefore match
- DTP defaults create trunks automatically whenever two switches are connected

Prevention—Reset any new switch's revision number to 0 by switching it to transparent mode and back or deleting the vlan.dat file before connecting it to the network.

VTP best practices

- If you're not going to use VTP, set each switch to transparent or off
- Any switch using VTP should have a (non-null) domain name and password
- If you're prototyping in a lab, always use a phony domain name and password
- Disable trunking on all switchports that you don't want to be trunks so a bad person can't deliberately cause a nuclear winter.

```
S2(config-if)# switchport mode access
S2(config-if)# switchport nonegotiate
```