Dynamic Trunking Protocol vs VLAN Trunking Protocol

- Topics covered:
    - Dynamic Trunking Protocol
    - VLAN Trunking Protocol

Dynamic Trunking Protocol (DTP)

- **What is Dynamic Trunking Protocol.**

  DTP is a Cisco proprietary protocol.
  It allows Cisco switches to negotiate whether a switchport should operate as an access port or a trunk port, without manual configuration.

- **What DTP does.**

  With DTP:

  - Two Cisco switches connected together can automatically form a trunk
  - Otherwise, the interface will operate as an access port

  Important points:

  - DTP is enabled by default on Cisco switch interfaces
  - Because it is Cisco proprietary, it works only between Cisco switches

- **Manual configuration vs DTP.**

  So far, switchports were manually configured using:

  - SWITCHPORT MODE ACCESS
  - SWITCHPORT MODE TRUNK

  If DTP is used:

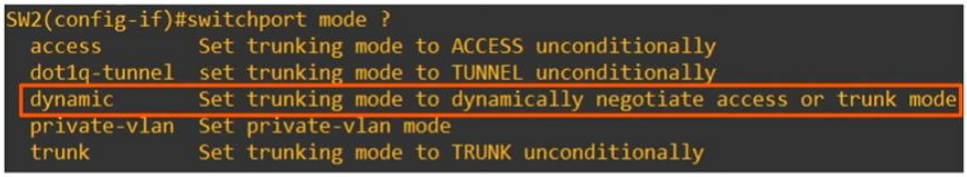
  - These commands are not required

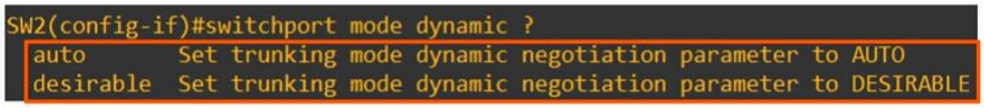
However:

- For security purposes, manual configuration is recommended
- DTP should be disabled on all switchports
- DTP can be exploited by attackers
- Network security will be discussed later

- **Let's go straight into the CLI.**

CLI output (shown once):





Explanation:

- The DYNAMIC option is DTP
- It dynamically negotiates access or trunk mode
- There are two dynamic modes:
  - **AUTO**
  - **DESIRABLE**

- **Understanding dynamic desirable mode.**

A switchport in dynamic desirable mode:

- Actively tries to form a trunk
- Sends DTP messages to the neighbour

It will form a trunk if the connected interface is in:

- switchport mode trunk
- switchport mode dynamic desirable

- switchport mode dynamic auto

Example 1: Dynamic desirable + Trunk.

Topology:

- SW1 G0/0 → dynamic desirable
- SW2 G0/0 → trunk

Result:

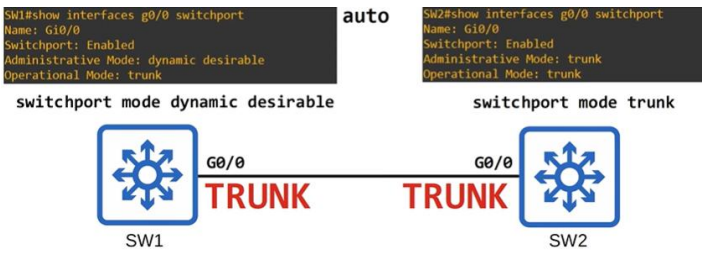
- A trunk is formed

Explanation:

- SW1 actively requests a trunk
- SW2 is already a trunk
- Both operate as trunk ports

SHOW INTERFACES SWITCHPORT command.

This command shows:



- **Administrative mode** → what was configured
- **Operational mode** → what the port is actually doing

Key point:

- Even a manually configured trunk still sends DTP frames

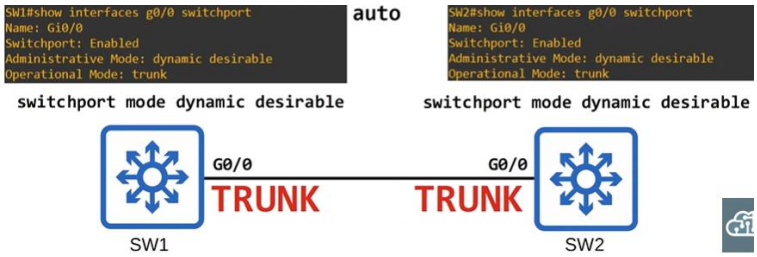
Example 2: Dynamic desirable + Dynamic desirable.

Topology:

- SW1 G0/0 → dynamic desirable
- SW2 G0/0 → dynamic desirable

Result:

- A **trunk is formed**



Explanation:

- Both switches actively try to form a trunk
- DTP negotiation succeeds
- Operational mode becomes **trunk**

Example 3: Dynamic desirable + Dynamic auto.

Dynamic auto behaviour:

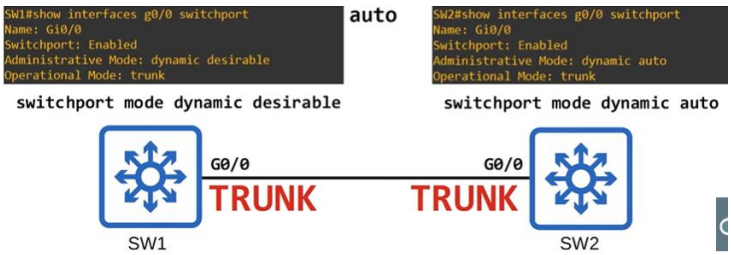
- Does not actively try to form a trunk
- Is passive
- Will form a trunk only if the other side requests it

Topology:

- SW1 G0/0 → dynamic desirable
- SW2 G0/0 → dynamic auto

Result:

- A trunk is formed



Explanation:

- SW1 actively requests a trunk
- SW2 agrees passively
- Operational mode is trunk

Example 4: Dynamic desirable + Access.

Topology:

- SW1 G0/0 → dynamic desirable
- SW2 G0/0 → access

Result:

- No trunk
- Both operate as access ports
- Default VLAN → VLAN 1

Explanation:

- Access mode is manually forced
- DTP negotiation cannot override it

What does “static access” mean?

Static access:

- An access port
- Belongs to one VLAN

- VLAN does not change unless manually reconfigured

Note:

- Dynamic access ports exist
- VLAN is assigned based on MAC address
- This is out of CCNA scope

- **Now let's look at dynamic auto mode.**

A switchport in dynamic auto mode:

- Does NOT actively try to form a trunk
- Will form a trunk only if the other side is active

It will form a trunk with:

- switchport mode trunk
- switchport mode dynamic desirable

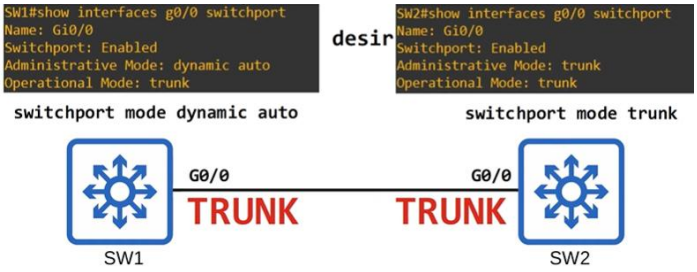
Example 1: Dynamic auto + Trunk.

Topology:

- SW1 G0/0 → dynamic auto
- SW2 G0/0 → trunk

Result:

- A **trunk is formed**



Explanation:

- SW2 actively runs trunk
- SW1 agrees passively

Example 2: Dynamic auto + Dynamic desirable.

Topology:

- SW1 G0/0 → dynamic auto
- SW2 G0/0 → dynamic desirable

Result:

- A trunk is formed

Explanation:

- SW2 actively requests
- SW1 accepts

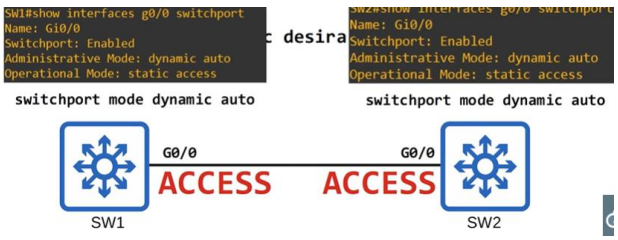
Example 3: Dynamic auto + Dynamic auto.

Topology:

- SW1 G0/0 → dynamic auto
- SW2 G0/0 → dynamic auto

Result:

- No trunk
- Both become access ports
- VLAN → VLAN 1



Explanation:

- Neither side actively requests a trunk

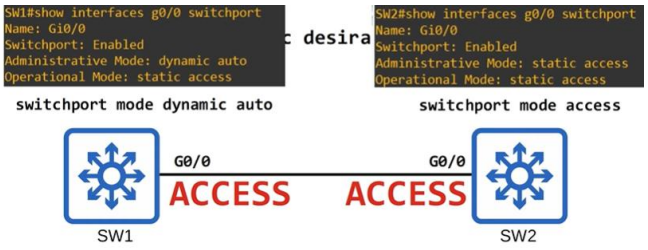
Example 4: Dynamic auto + Access.

Topology:

- SW1 G0/0 → dynamic auto
- SW2 G0/0 → access

Result:

- **Access mode**



Explanation:

- Access mode is forced
- No trunk negotiation occurs

Example 5: Manual trunk + manual access.

Topology:

- One side → switchport mode trunk
- Other side → switchport mode access

Result:

- Mismatch
- Traffic will not pass correctly
- This configuration is broken

- **DTP summary table (operational result).**

Administrative Mode	Trunk	Dynamic Desirable	Access	Dynamic Auto
Trunk	Trunk	Trunk	X	Trunk
Dynamic Desirable	Trunk	Trunk	Access	Trunk
Access	X	Access	Access	Access
Dynamic Auto	Trunk	Trunk	Access	Access

Meaning:

- Dynamic desirable forms a trunk with everything except access
- Dynamic auto forms a trunk only if the other side is active

- **Note That.**

DTP:

- Will NOT form a trunk with:
  - Routers
  - PCs
  - Non-Cisco devices

Therefore:

- For router on a stick
- You must manually configure the switchport as a trunk
- Dynamic desirable will not work in this case

- **Let me cover a few more points about DTP.**

On older switches:

- switchport mode **dynamic desirable is the default administrative mode**
- Interfaces actively try to form trunk links

On newer switches:

- switchport mode **dynamic auto is the default administrative mode**
- Interfaces are passive and do not actively try to form trunks

- **Disabling DTP negotiation.**

  You can disable DTP on an interface using:

  - “switchport no negotiate”

  What this does:

  - Stops the interface from sending DTP frames
  - DTP negotiation is disabled

- **Access mode and DTP.**

  If you configure:

  - switchport mode access

  Then:

  - DTP negotiation is automatically disabled
  - The interface stops sending DTP frames

- **Trunk mode and DTP.**

  If you configure:

  - switchport mode trunk

  Then:

  - The interface still sends DTP frames
  - DTP is not disabled automatically

  To fully disable DTP on a trunk port:

  - You must also use “switchport no negotiate”

- **Recommended best practice.**

  It is recommended to:

  - Disable DTP on all switchports
  - Manually configure ports as access or trunk

- **Trunk encapsulation negotiation.**

  Some switches support:

  - **dot1q**
  - **ISL**

  These switches can use DTP to negotiate which encapsulation to use.

  The default setting is:

  - switchport trunk encapsulation negotiate

  This allows the switch to:

  - Automatically choose the encapsulation type

- **Manual trunk encapsulation configuration.**

  If you want to manually configure a trunk on a switch that supports both:

  - You **cannot** leave encapsulation in negotiate mode
  - You must explicitly configure:
    - “switchport trunk encapsulation dot1q”
    - or
    - “switchport trunk encapsulation isl”

- **ISL vs dot1q selection.**

  Rules:

  - ISL is preferred over dot1q
  - If both switches support ISL, ISL will be selected

- **Where DTP frames are sent.**

  DTP frames are sent:

  - In VLAN 1 when using ISL
  - In the native VLAN when using dot1q

  Default:

  - Native VLAN = VLAN 1

  So unless changed:

  - DTP frames are sent in VLAN 1 for both ISL and dot1q

- **CLI output (shown once).**

```
SW1(config-if)#switchport mode dynamic desirable
SW1(config-if)#do show interfaces g0/0 switchport
Name: Gi0/0
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: trunk
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: isl
Negotiation of Trunking: On
```

```
SW2(config-if)#switchport mode dynamic desirable
SW2(config-if)#do show interfaces g0/0 switchport
Name: Gi0/0
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: trunk
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: isl
Negotiation of Trunking: On
```

  Explaining the output:

  - Administrative Mode
    - What was configured on the interface
    - Here: dynamic desirable
  - Operational Mode
    - What the interface is actually doing
    - Here: trunk
  - Administrative Trunking Encapsulation
    - Set to negotiate by default
  - Operational Trunking Encapsulation

        - Result of negotiation
        - Here: isl
    - Negotiation of Trunking: On
        - DTP is enabled
        - DTP frames are being sent

- **When is “Negotiation of Trunking” ON or OFF.**

  It is **ON** when the interface is in:

  - dynamic desirable
  - dynamic auto
  - trunk mode

  It is **OFF** when the interface is in:

  - access mode
  - or when “switchport no negotiate” is used

  Okay, that was a good deal of information about DTP.

VTP (VLAN Trunking Protocol)

- **What is VLAN Trunking Protocol.**

VTP allows you to configure VLANs on a central server switch.
Other switches, called VTP clients, will synchronize their VLAN database to the server.

It is designed for large networks with many VLANs, so you don't have to configure VLANs on every switch.

However:

- Like DTP, it is rarely used
- It is recommended that you do not use it
- One important reason will be shown later

- **VTP versions.**

  There are three versions of VTP:

  - VTP version 1
  - VTP version 2
  - VTP version 3

  Most modern Cisco switches support all three.
  Older switches might support only version 1 and 2.

- **VTP modes.**

  There are three VTP modes:

  - Server
  - Client
  - Transparent

  Cisco switches operate in VTP server mode by default.

- **VTP server mode.**

  VTP servers:

  - Can add VLANs
  - Can modify VLANs
  - Can delete VLANs

  They store the VLAN database in NVRAM.

  - The VLAN database is saved even if the switch is reloaded or powered off

  Every time a VLAN is:

  - Added
  - Modified
  - Deleted

  The revision number increases.

  The VTP revision number:

  The revision number is very important.

  VTP uses it to:

  - Decide which VLAN database is the newest
  - Decide which database switches should synchronize to

  The highest revision number always wins.

  How VTP advertisements work.

  - VTP servers send advertisements **only on trunk ports**
  - VTP advertisements are **not sent on access ports**
  - VTP clients synchronize their VLAN database to the server

  Important:

  - VTP servers also function as VTP clients
  - A VTP server will synchronize to another server with a higher revision number

- **VTP client mode.**

  VTP clients:

  - **Cannot** add VLANs
  - **Cannot** modify VLANs
  - **Cannot** delete VLANs

  If you try, the CLI command will be rejected.

  They normally:

  - Do not store the VLAN database in NVRAM
  - In VTPv3, they do store it

  They:

  - Synchronize to the server with the highest revision number
  - Forward VTP advertisements over trunk ports

- **Basic topology.**

  All interfaces are configured as trunks, so VTP advertisements can pass between them.

  CLI output :

```
SW1#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0c09.f956.1300
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN:
--------------
VTP Operating Mode              : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 5
Configuration Revision          : 0
MD5 digest                      : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
                                  0x56 0x9D 0x4A 0x3E 0xA5 0x69 0x35 0xBC
```

  Explaining the default VTP status:

  - VTP version running is 1 (default)
  - Domain name is NULL

- Operating mode is Server
- Maximum VLANs is 1005

Reason:

- VTP version 1 and 2 do not support extended VLANs (1006–4094)
- Only VTPv3 supports extended VLANs

Existing VLANs:

- VLAN 1
- VLAN 1002–1005 (default VLANs)

Revision number:

- Starts at 0

Configuring a VTP domain and VLAN.

On SW1:

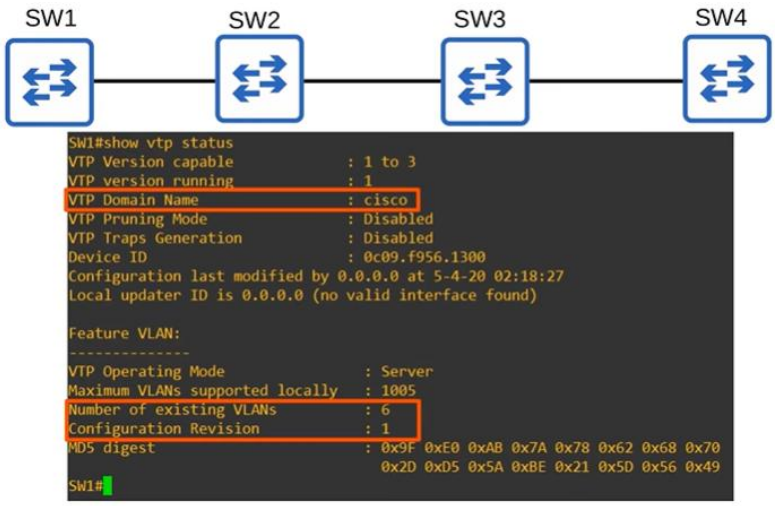
```
SW1(config)#vtp domain cisco
Changing VTP domain name from NULL to cisco
SW1(config)#
*May  4 02:14:47.276: %SW_VLAN-6-VTP_DOMAIN_NAME_CHG: VTP domain name changed to cisco.
SW1(config)#vlan 10
SW1(config-vlan)#name engineering
SW1(config-vlan)#exit
```

- I configure the VTP domain name to cisco
- I create VLAN 10
- I name it engineering

Because a VLAN was added:

- The revision number increases

Verifying VTP after adding a VLAN.



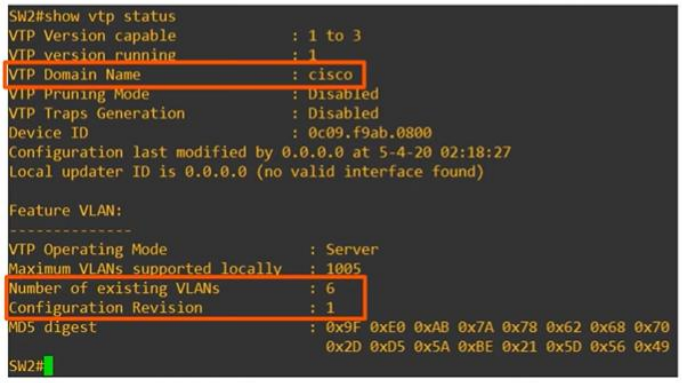
Explanation:

- Domain name changed to **cisco**
- VLAN count increased
- Revision number increased to **1**

What happened on SW2?

Without any configuration on SW2:

- The VTP domain name changed to cisco
- VLAN 10 was added automatically
- Revision number became 1



Important rule:

- If a switch with NULL domain receives a VTP advertisement
- It will automatically join that VTP domain

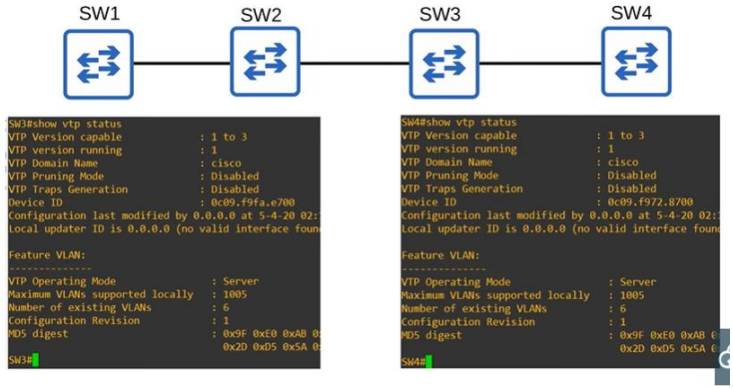
Verifying VLANs on SW2.

This confirms:

- VTP synchronization worked
- VLAN database was copied from SW1

VTP propagation to other switches.

SW3 and SW4:



- Also received the VTP advertisement
- Joined the **cisco** domain
- Updated their VLAN databases

VTP advertisements were forwarded across the trunk links.

The major danger of VTP.

If you connect:

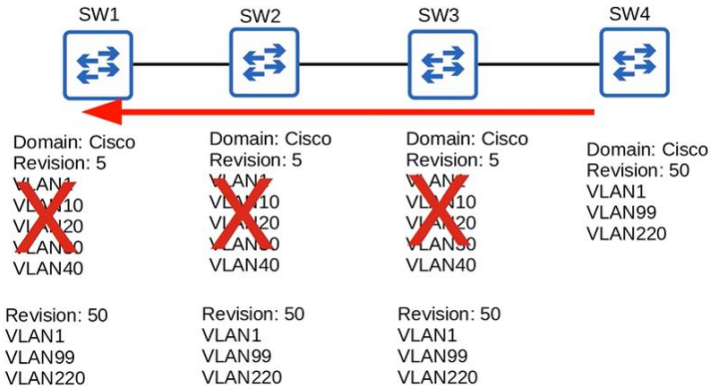
- An old switch

- With the same VTP domain name
- But a higher revision number

Then:

- All switches will synchronize to that database
- Even if it is wrong

Dangerous scenario.



What happens in this case:

Because:

- Revision 50 is higher than 5

All switches will:

- Synchronize to VLANs 1, 99, and 220
- VLANs 10, 20, 30, 40 disappear

Result:

- Hosts instantly lose connectivity

- **Why VTP is not recommended.**

  Because:

  - One wrong switch
  - One higher revision number

  Can:

  - Destroy the entire VLAN database
  - Cause a network-wide outage

- **VTP transparent mode.**

Switches in VTP transparent mode do not participate in the VTP domain.
They do not synchronize their VLAN database to the VTP server.

They maintain their own independent VLAN database, which is stored in NVRAM.

They can add, modify, and delete VLANs, but those VLANs are not advertised to other switches.

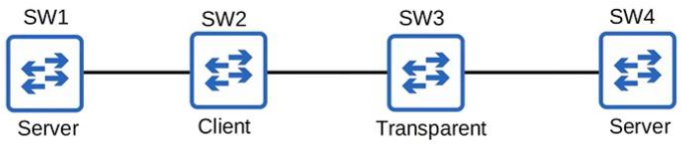
- **Forwarding behaviour in transparent mode.**

  Although a transparent switch does not sync its VLAN database:

  - It will forward VTP advertisements
  - Only if the advertisement is in the same VTP domain

  It will not advertise its own VLAN database.

- **Topology used in this lab.**



All links are trunk links.

Setting SW2 to VTP client mode (CLI shown once).

```
SW2(config)#vtp mode client
Setting device to VTP Client mode for VLANS.
SW2(config)#vlan 20
VTP VLAN configuration not allowed when device is in CLIENT mode.
SW2(config)#
```

Explanation:

- VTP clients cannot create VLANs
- Any VLAN configuration command is rejected

Setting SW3 to VTP transparent mode.

```
SW3(config)#vtp mode transparent
Setting device to VTP Transparent mode for VLANS.
SW3(config)#vtp domain juniper
Changing VTP domain name from cisco to juniper
SW3(config)#
```

Explanation:

- SW3 is now transparent
- Domain is changed to juniper
- This will affect VTP forwarding behaviour

Creating VLAN20 on the VTP server (SW1).

```
SW1(config)#vlan 20
SW1(config-vlan)#name sales
SW1(config-vlan)#exit
SW1(config)#do show vlan brief

VLAN Name                              Status    Po
---- --------------------------------- --------- --
1    default                           active    Gi
                                                 Gi
                                                 Gi
                                                 Gi
10   engineering                       active
20   sales                             active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
SW1(config)#
```

Verifying revision number on SW1.

```
SW1(config)#do show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : cisco
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0c09.f956.1300
Configuration last modified by 0.0.0.0 at 5-4-20 03:40:01
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN:
--------------
VTP Operating Mode              : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 7
Configuration Revision          : 4
MD5 digest                      : 0x8F 0x9C 0x81 0x4B 0x
                                  0xE8 0xA3 0x98 0xFD 0x
SW1(config)#
```

Explanation:

- VLAN was added
- Revision number increased
- SW1 advertises this to the VTP domain

Checking the VTP client (SW2).

```
SW2#show vlan brief

VLAN Name                              Status    P
---- --------------------------------- --------- -
1    default                           active    G
                                                 G
                                                 G
                                                 G
10   engineering                       active
20   sales                             active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
SW2#
```

```
SW2#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : cisco
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0c09.f9ab.0800
Configuration last modified by 0.0.0.0 at 5-4-20 03:40:01

Feature VLAN:
--------------
VTP Operating Mode              : Client
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 7
Configuration Revision          : 4
MD5 digest                      : 0x8F 0x9C 0x81 0x4B 0x
                                  0xE8 0xA3 0x98 0xFD 0x
SW2#
```

Explanation:

- SW2 automatically synchronized

- VLAN20 was added
- Revision number matches the server

Checking the transparent switch (SW3).

Explanation:

- Transparent switches do not sync VLANs
- Changing to transparent mode resets revision to 0
- Changing VTP domain also resets revision to 0

Why revision reset is important.

If you connect:

- An old switch
- With a high revision number

You must:

- Change VTP domain or
- Set it to transparent

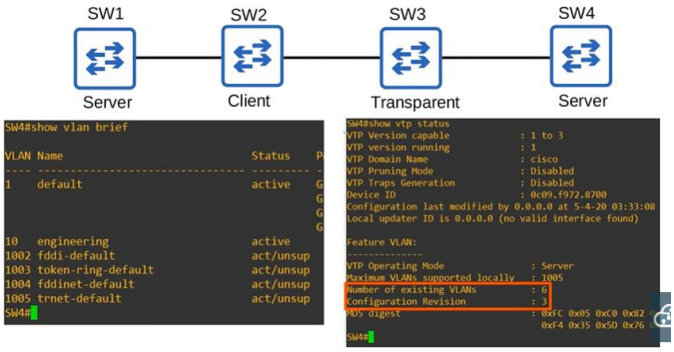
This prevents it from overwriting the network VLAN database.

Checking SW4 behaviour (image scenario).

Current situation (ASCII):

SW1 -------- SW2 -------- SW3 -------- SW4

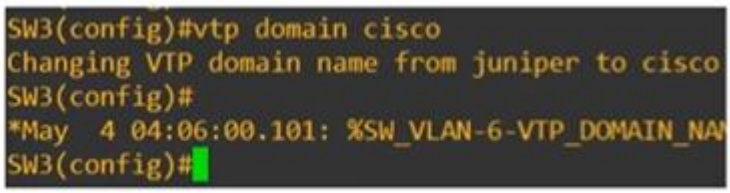
Server Client Transparent(juniper) Server



Result:

- SW3 does not forward VTP advertisements
- SW4 does not receive VLAN20
- Revision remains unchanged

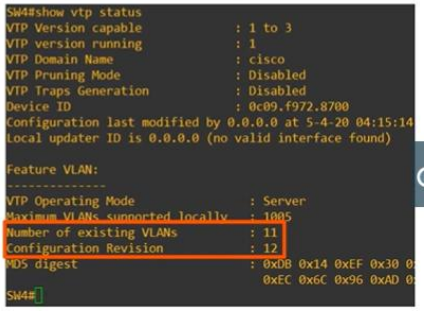
Making SW3 forward VTP advertisements.



Explanation:

- SW3 is still transparent
- But now in the same domain
- It will forward advertisements

Verifying SW4 after forwarding resumes.

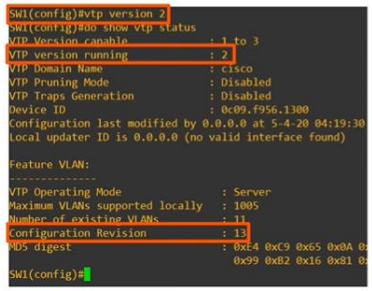


Explanation:

- SW4 received VTP advertisements
- VLAN database synchronized
- Revision number updated

Changing VTP version.

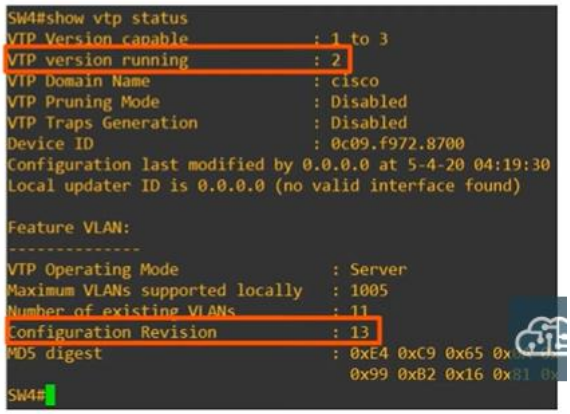
SW1(config)#vtp version 2



Effect:

- Revision number increases
- Advertisements are sent
- Other switches synchronize

Verification (example):



- **Difference between VTP version 1 and 2.**

  According to Cisco:

  - VTP v2 is not much different from v1
  - Main difference:
    - Support for Token Ring VLANs

  If you don’t use Token Ring:

  - There is no reason to use v2

- **About VTP version 3.**

  VTP version 3:

  - Has many new features
  - Is beyond CCNA scope

  So we stop here.