DTP and VTP - Cisco Proprietary Protocols

Dynamic Trunking Protocol (DTP)

DTP is a **Cisco proprietary protocol** that allows Cisco switches to dynamically negotiate the status of an interface – **access** or **trunk** – without manual configuration. It is enabled by default on all Cisco switch interfaces. For security, manual configuration is recommended and DTP should be disabled on all switchports.

DTP Modes

Switch interfaces can be configured in one of several administrative modes. The two DTP-specific modes are:

```
SW2(config-if)#switchport mode ?
  access        Set trunking mode to ACCESS unconditionally
  dot1q-tunnel  set trunking mode to TUNNEL unconditionally
  dynamic       Set trunking mode to dynamically negotiate access or trunk mode
  private-vlan  Set private-vlan mode
  trunk         Set trunking mode to TRUNK unconditionally
```

- **Dynamic Desirable** (it's the "**asker**") – Actively tries to form a trunk. Will form a trunk if the neighboring interface is in any of these modes:
  - `switchport mode trunk`
  - `switchport mode dynamic desirable`
  - `switchport mode dynamic auto`
  - **Will not** form a trunk if connected to a switchport in access mode
- **Dynamic Auto** (it's the "**responder**") – Passively waits for trunk negotiation. Will form a trunk only if the neighboring interface is actively trying (i.e., in `trunk` or `dynamic desirable` mode). It will *not* initiate negotiation

```
SW2(config-if)#switchport mode dynamic ?
  auto       Set trunking mode dynamic negotiation parameter to AUTO
  desirable  Set trunking mode dynamic negotiation parameter to DESIRABLE
```

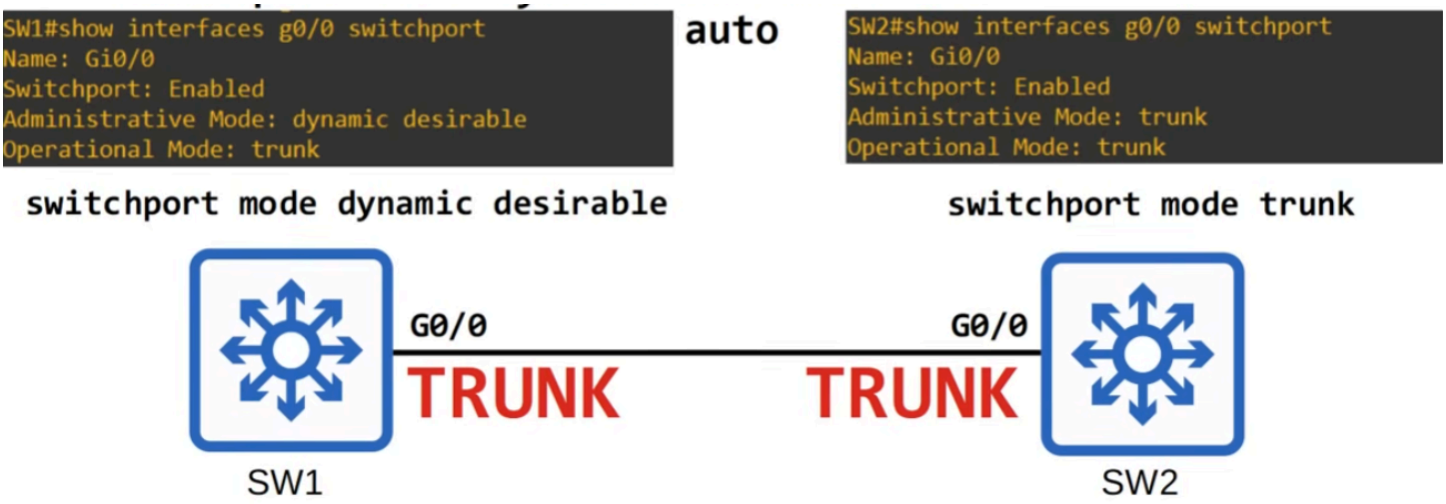
- Forms a trunk with:
  - `switchport mode trunk`
  - `switchport mode dynamic desirable`
  - **Will not** form a trunk with another `dynamic auto` interface (both passive → access port)

Other manual modes are:

- **Access** – Manually set as an access port. Disables DTP negotiation.
- **Trunk** – Manually set as a trunk. DTP frames are still sent; to stop sending them, use `switchport nonegotiate`.

CLI Examples and `show interfaces switchport` Output

Example 1: Dynamic Desirable ↔ Trunk



- **SW1 G0/0**: `dynamic desirable`
- **SW2 G0/0**: manually configured as `trunk`

Result: Both form a trunk.

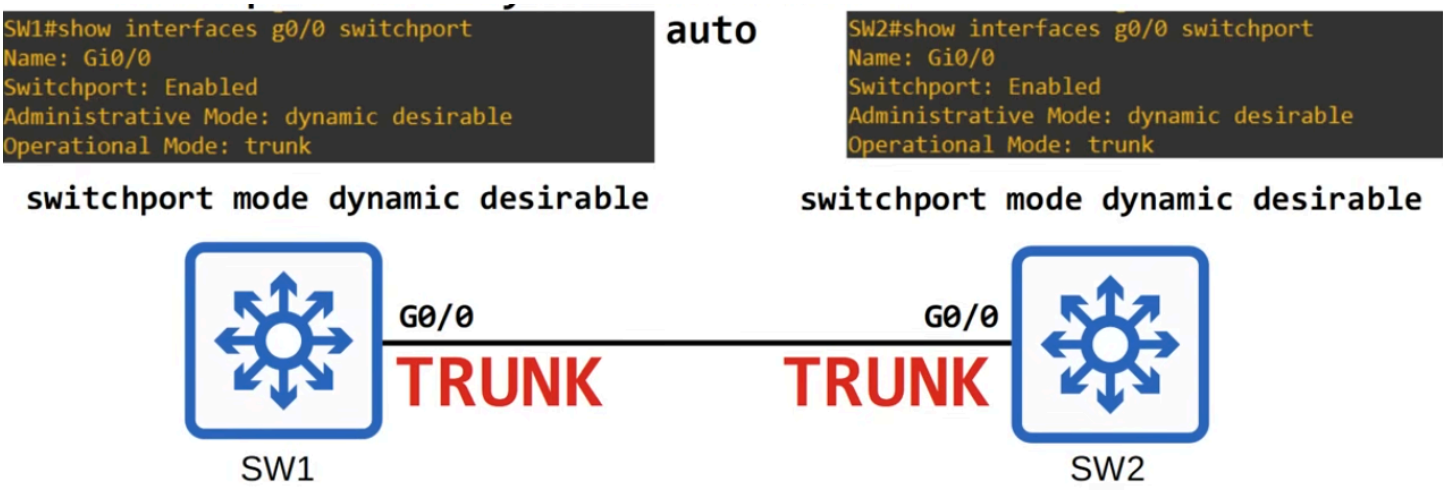
SW1 output (partial):

```
Administrative Mode: dynamic desirable
Operational Mode: trunk
```

SW2 output:

```
Administrative Mode: trunk
Operational Mode: trunk
```

Example 2: Dynamic Desirable ↔ Dynamic Desirable



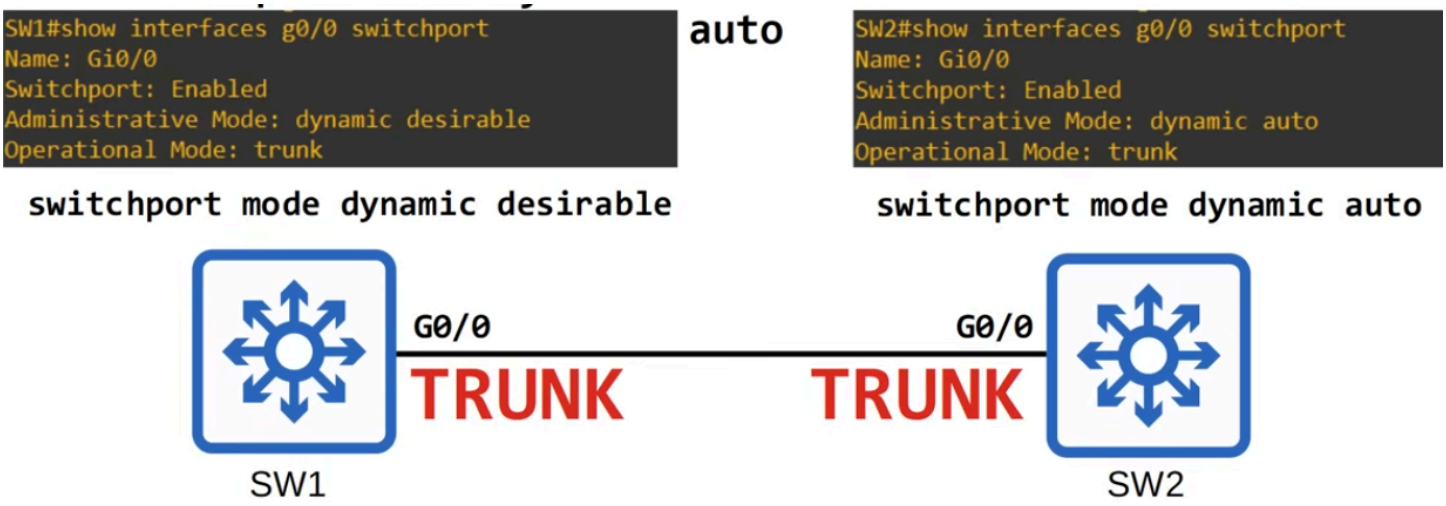
- **SW1 G0/0**: `dynamic desirable`
- **SW2 G0/0**: `dynamic desirable`

Result: Both form a trunk.

SW2 output:

```
Administrative Mode: dynamic desirable
Operational Mode: trunk
```

Example 3: Dynamic Desirable ↔ Dynamic Auto



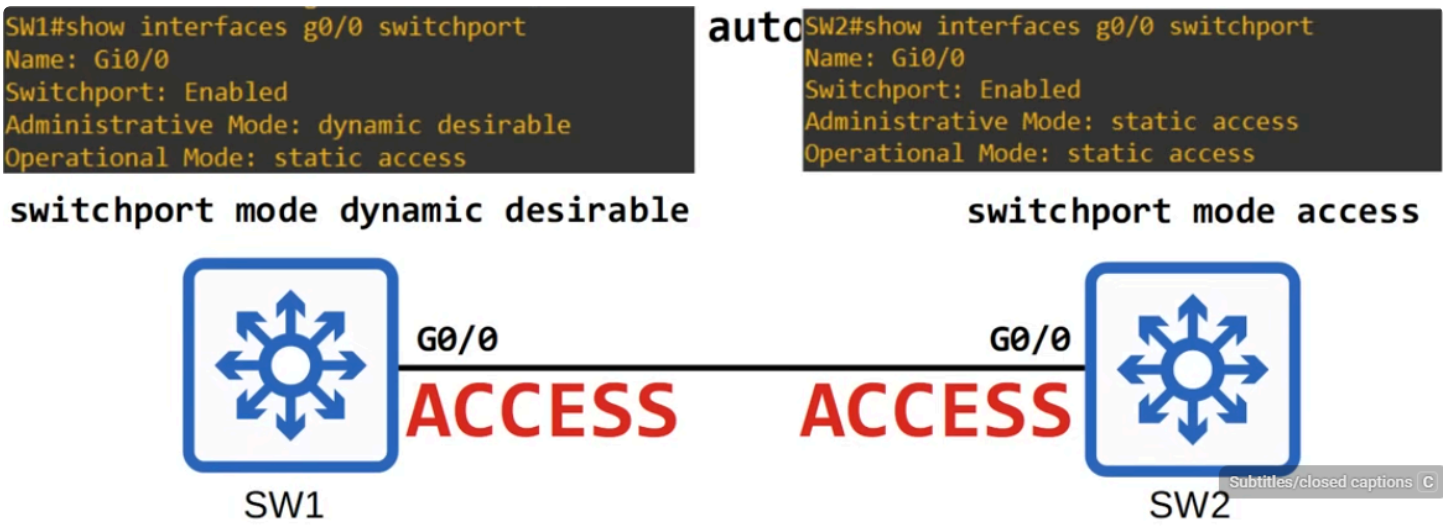
- **SW1 G0/0**: `dynamic desirable`
- **SW2 G0/0**: `dynamic auto`

Result: Both form a trunk (SW1 actively tries; SW2 accepts). Since the SW2 interface is in dynamic auto mode, it does not actively try to form a trunk. It's more passive. It will tell SW1 if you want to form a trunk. I'll form a trunk, but I'm not going to actively form a trunk with you.

SW2 output:

```
Administrative Mode: dynamic auto
Operational Mode: trunk
```

Example 4: Dynamic Desirable ↔ Access



- **SW1 G0/0**: `dynamic desirable`
- **SW2 G0/0**: manually configured as `switchport mode access`

Result: Both operate as access ports in the default VLAN (VLAN 1). Trunk is **not** formed. SW1 is actively trying to form a trunk, but since SW2 is manually configured in access mode, the trunk will not form, and both will operate as access port in the default VLAN, which is VLAN 1.

SW1 output:

```
Administrative Mode: dynamic desirable
Operational Mode: static access
```

> ***Note:*** `static access` ***means an access port that belongs to a single fixed VLAN (as opposed to*** `dynamic access` ***where a server assigns the VLAN based on MAC address — out of CCNA scope).***

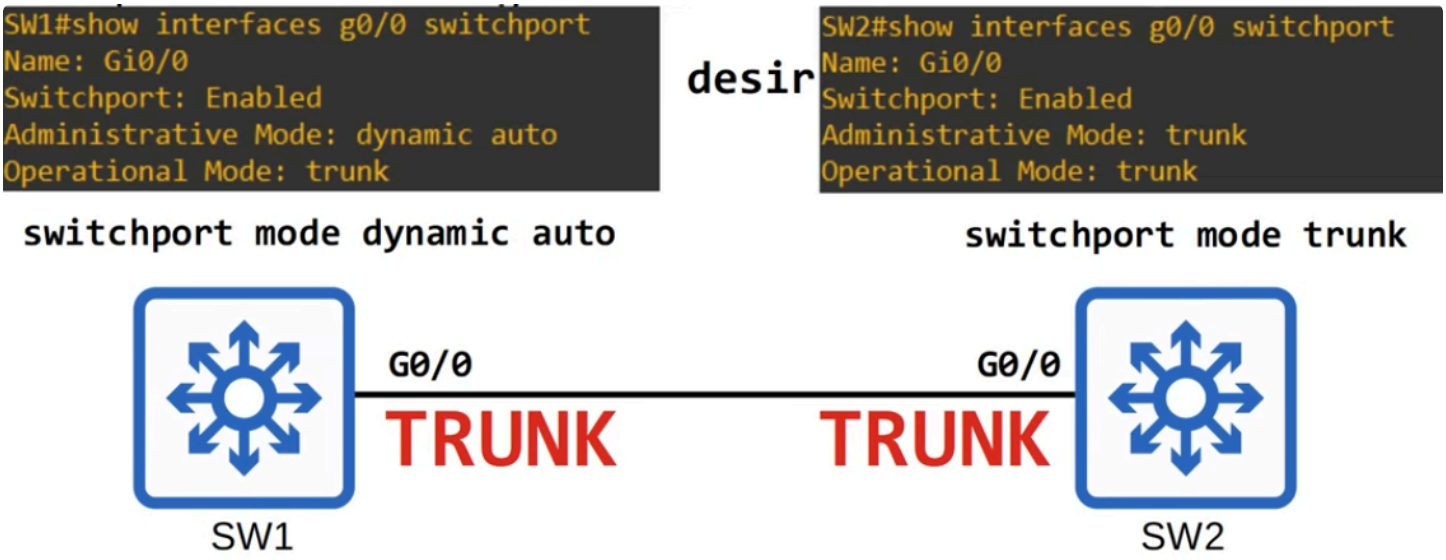
SW2 output:

```
Administrative Mode: static access
Operational Mode: static access
```

Dynamic Auto Mode Examples

- **Dynamic Auto** = passively waits for the other side to ask (it's the "**responder**")

Example 5: Dynamic Auto ↔ Trunk



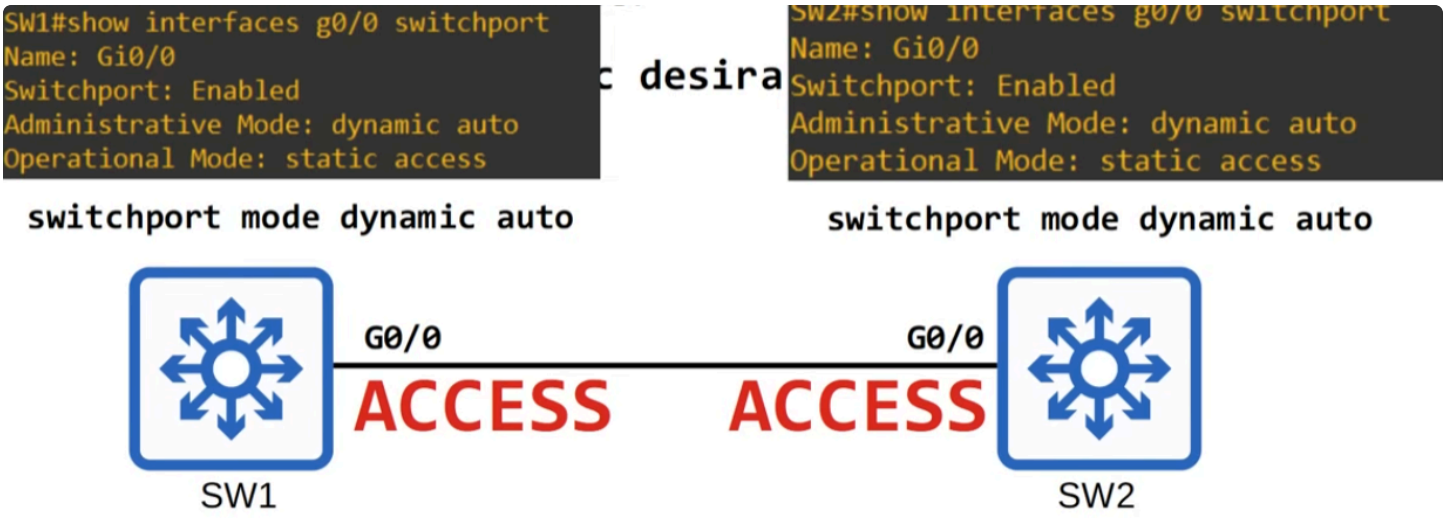
- **SW1 G0/0**: `dynamic auto`
- **SW2 G0/0**: manually configured as `trunk`

Result: Both form a trunk.

SW1 output:

```
Administrative Mode: dynamic auto
Operational Mode: trunk
```

Example 6: Dynamic Auto ↔ Dynamic Auto



- **SW1 G0/0**: `dynamic auto`
- **SW2 G0/0**: `dynamic auto`

Result: Both operate as access ports. Neither is actively trying to form a trunk.

SW1 and SW2 output (same on both):

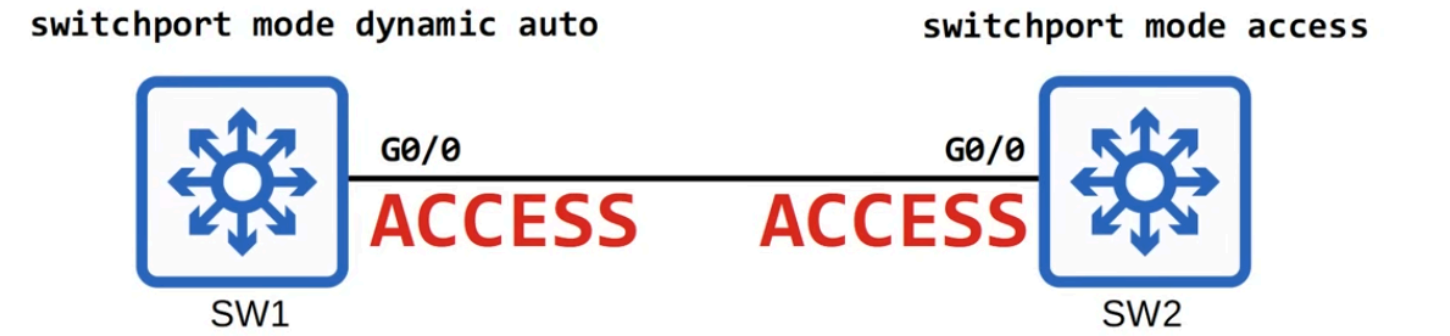
```
 Administrative Mode: dynamic auto
Operational Mode: static access
```

Example 7: Dynamic Auto ↔ Access

```
SW1#show interfaces g0/0 switchport
Name: Gi0/0
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
```

c desira

```
SW2#show interfaces g0/0 switchport
Name: Gi0/0
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
```



- **SW1 G0/0**: `dynamic auto`
- **SW2 G0/0**: `switchport mode access`

Result: Both operate as access ports.

(Output similar to Example 6)

Misconfiguration Example

Trunk ↔ Access (Do Not Use)

```
SW1#show interfaces g0/0 switchport
Name: Gi0/0
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
```

```
SW2#show interfaces g0/0 switchport
Name: Gi0/0
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
```

- **SW1 G0/0**: manually configured as `trunk`

- **SW2 G0/0**: manually configured as `access`

Result: Operational mismatch — `trunk` on one end, `access` on the other. Traffic will **not** pass between these switches. This configuration results in an error.

```
SW1 output: Administrative Mode: trunk, Operational Mode: trunk
SW2 output: Administrative Mode: static access, Operational Mode: static access
```

Important DTP Rules

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

Additional DTP Facts

- DTP will **not** form a trunk with a router, PC, or any non-Cisco device. The switchport will remain in access mode.
- For **router-on-a-stick**, the switch interface connected to the router must be **manually configured as a trunk**.

- On **older switches**: default administrative mode is `dynamic desirable`.
- On **newer switches**: default administrative mode is `dynamic auto`.
- **Default VLAN**: Unless otherwise configured, all switchports that are in access mode operate in **VLAN 1**.
- The `switchport nonegotiate` command stops the interface from sending DTP frames.
- Manually configuring `switchport mode access` also disables DTP negotiation.
- Manually configuring `switchport mode trunk` does **not** disable DTP; DTP frames continue to be sent unless `switchport nonegotiate` is also applied.

Default DTP Mode and Disabling DTP

- **Older switches**: default administrative mode is **dynamic desirable**.
- **Newer switches**: default administrative mode is **dynamic auto**.
- To disable DTP negotiation on an interface, use the command: `switchport nonegotiate`. This stops the interface from sending DTP frames.
- Manually configuring an interface as an access port (`switchport mode access`) also disables DTP.
- Configuring an interface as a trunk does **not** disable DTP unless `switchport nonegotiate` is also applied.

Trunk Encapsulation Negotiation

On switches that support both **dot1q** and **ISL** trunk encapsulations, DTP can negotiate which encapsulation to use. The default mode is `switchport trunk encapsulation negotiate`. ISL is favored over dot1q if both ends support it. If DTP negotiation is used, the operational encapsulation is determined by the negotiation.

- DTP frames are sent in VLAN 1 when using ISL, or in the native VLAN (default VLAN 1) when using dot1q.

CLI Demonstration

Setup: Both SW1 and SW2 interfaces are set to `dynamic desirable` mode so they form a trunk.

Command used to verify:

```
do show interfaces g0/0 switchport
```

```
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
```

Explanation of Each Field

Field	Meaning
`Trunking Encapsulation Mode`	What encapsulation mode is configured on the interface (`negotiate`, `dot1q`, or `isl`)
`Operational Trunking Encapsulation`	What encapsulation is actually being used after negotiation (`isl` in this example when both support ISL)
`Negotiation of Trunking`	Whether DTP is enabled on the interface (`on` or `off`)

DTP Status: When is Negotiation On or Off?

- **Negotiation of Trunking = ON** when the interface is in:
  - `dynamic desirable` mode
  - `dynamic auto` mode
  - `trunk` mode
- **Negotiation of Trunking = OFF** when the interface is in:
  - `access` mode
  - When `switchport nonegotiate` command has been applied

VLAN Trunking Protocol (VTP)

VTP is a **Cisco proprietary protocol** that allows configuration of VLANs on a central **VTP server** switch; other switches (**VTP clients**) synchronize their VLAN database to the server. It is designed for large networks but is rarely used in modern networks due to risks (see warning below). VTP operates only over trunk links.

VTP Modes

There are three modes:

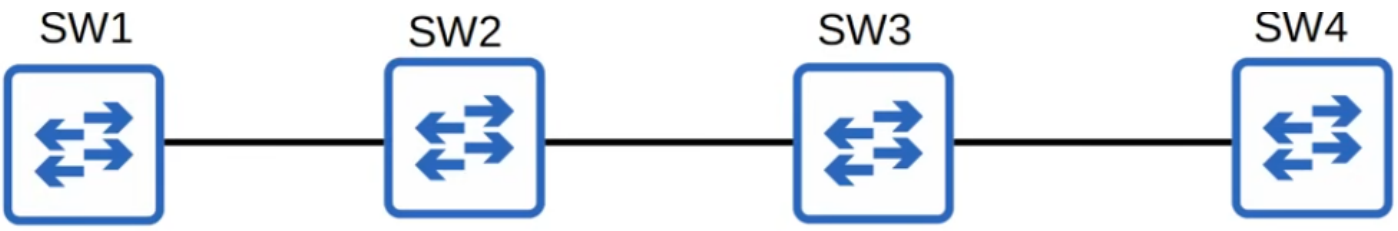
- **VTP Server** (default on Cisco switches)
  - Can add, modify, and delete VLANs.
  - Stores VLAN database in NVRAM (persistent across reboots).
  - Increases the **revision number** every time a VLAN is changed.
    - The **VTP revision number** is a counter that tracks the **version** of the VLAN database on a VTP server which is the newest most accurate version of the vlan database.
  - Advertises the VLAN database on trunk interfaces.
  - **Also functions as a client**: synchronizes to another vtp server with a higher revision number.

- **VTP Client**
  - Cannot add, modify, or delete VLANs – commands are rejected.
  - Synchronizes its VLAN database to the VTP server with the highest revision number in the same domain.
  - Does **not** store VLAN database in NVRAM (except in VTP version 3).
  - Advertises and forwards VTP advertisements over trunk ports.
- **VTP Transparent**
  - Does **not** participate in the VTP domain (maintains its own independent VLAN database in NVRAM).
  - Can add, modify, and delete VLANs locally, but does not advertise its own VLAN database.
  - **Forwards** VTP advertisements over trunk ports if the advertisement belongs to the same VTP domain as the transparent switch itself.

VTP Demonstration — Configuration and Synchronization

Network Setup

Four switches (SW1, SW2, SW3, SW4) are connected.



- All interfaces are configured as **trunks** so they can send and receive VTP advertisements.

Key Command: `show vtp status`

This is a very useful command to display VTP information on a switch.

Default `show vtp status` Output on SW1

```
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
```

Field	Value	Meaning
VTP Version (capable)	1, 2, or 3	Switch can run any of these versions
VTP Version (running)	1	Default version
VTP Domain Name	NULL	No domain name configured by default
VTP Operating Mode	Server	Default mode on Cisco switches
Maximum VLANs Supported	1005	VTP v1 and v2 do not support extended VLAN range (1006–4094) You will need to use v3 for extended range
Number of Existing VLANs	5	Default VLANs: 1, 1002, 1003, 1004, 1005
Configuration Revision	0	Default value — no VLAN changes made yet Adding, Modifying, or Deleting a VLAN can increase it's number

> ***Note: Only VTP version 3 supports the extended VLAN range (1006–4094).***

Step-by-Step Configuration

```
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
```

Step 1: Set VTP Domain on SW1

Command:

```
vtp domain cisco
```

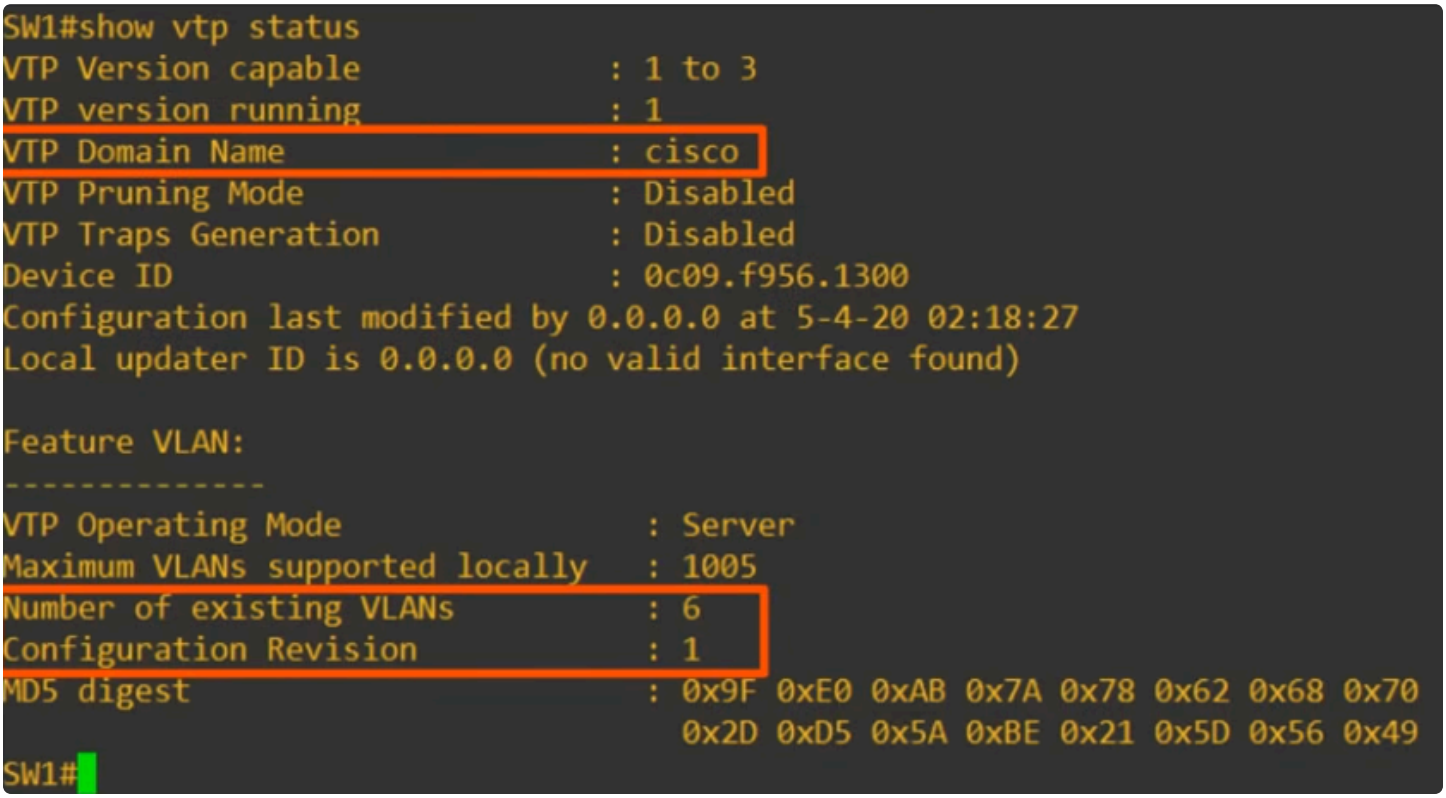
Result: SW1's VTP domain name is changed to `cisco`.

Step 2: Create a VLAN on SW1

Commands:

```
vlan 10
name engineering
```

Result on SW1 (`show vtp status`):

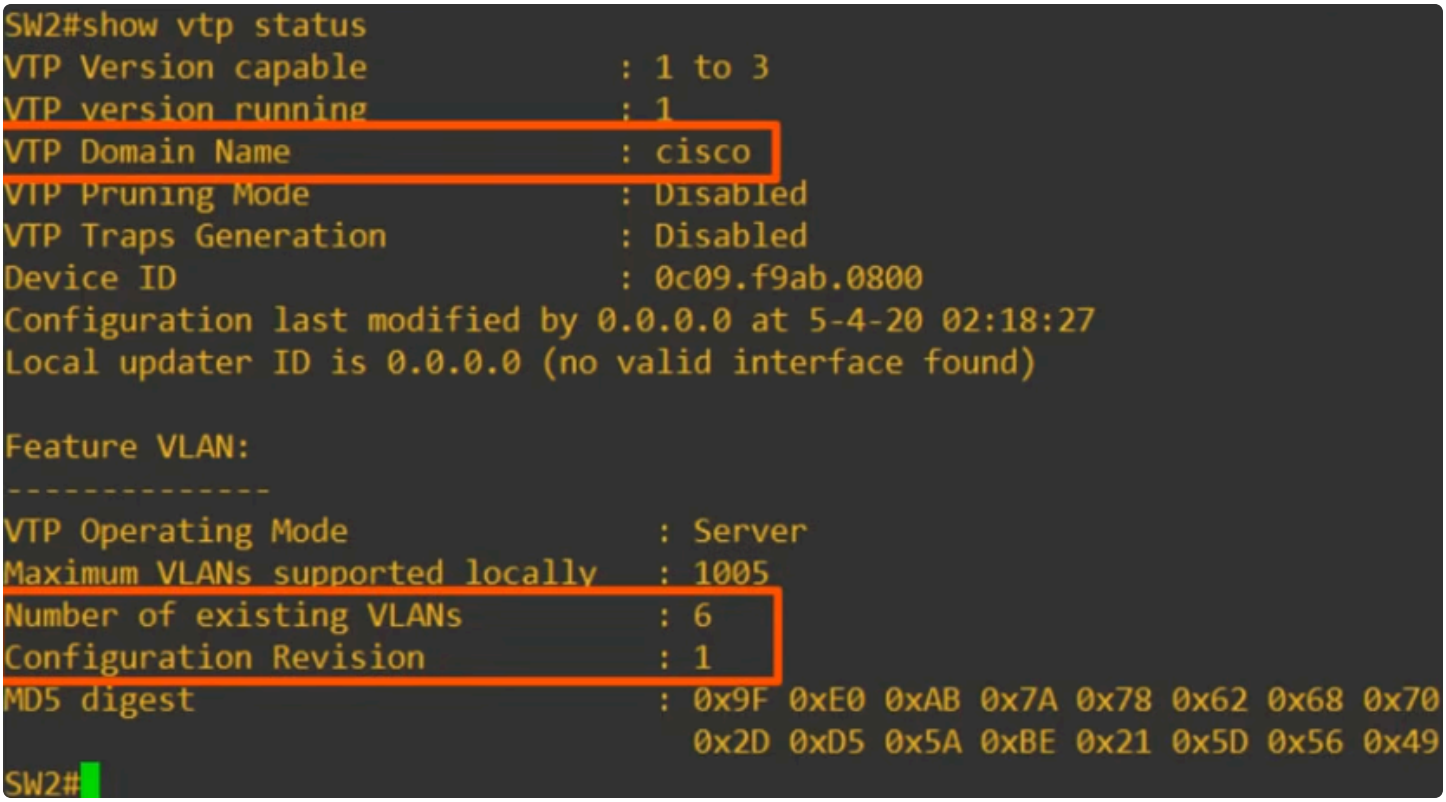


- VTP Domain Name: `cisco`
- Number of Existing VLANs: **6** (VLANs 1, 1002, 1003, 1004, 1005, and now VLAN 10)
- Configuration Revision: **1** (incremented from 0 because a VLAN was added)

Automatic Synchronization

SW2 Behavior

Without any manual configuration on SW2:



- SW2 automatically **joins the domain** `cisco`
- SW2 **updates its VLAN database** to match SW1's
- SW2 has revision number **1**

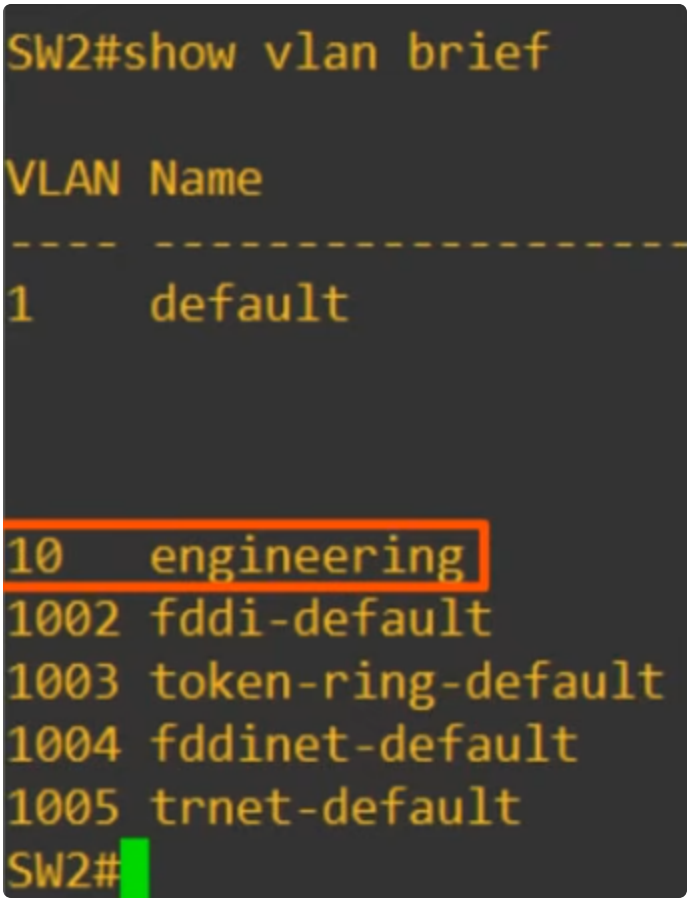
Why?

- If a switch with **no VTP domain** (domain NULL) receives a VTP advertisement with a VTP domain name, it will **automatically join** that VTP domain.
- If a switch receives a VTP advertisement in the **same VTP domain** with a **higher revision number**, it will **update its VLAN database** to match.

Verification on SW2

Command:

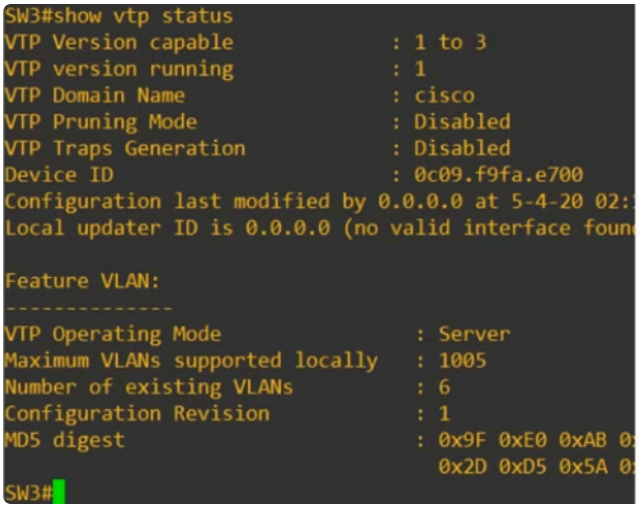
```
show vlan brief
```

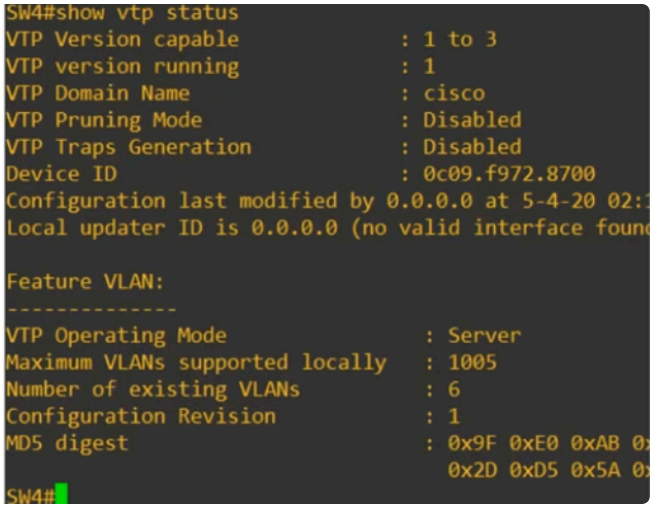


Result: VLAN 10, with the name `engineering`, is present on SW2 even though it was never configured locally.

SW3 and SW4 Behavior

The VTP advertisements are **passed along** through the trunk links:



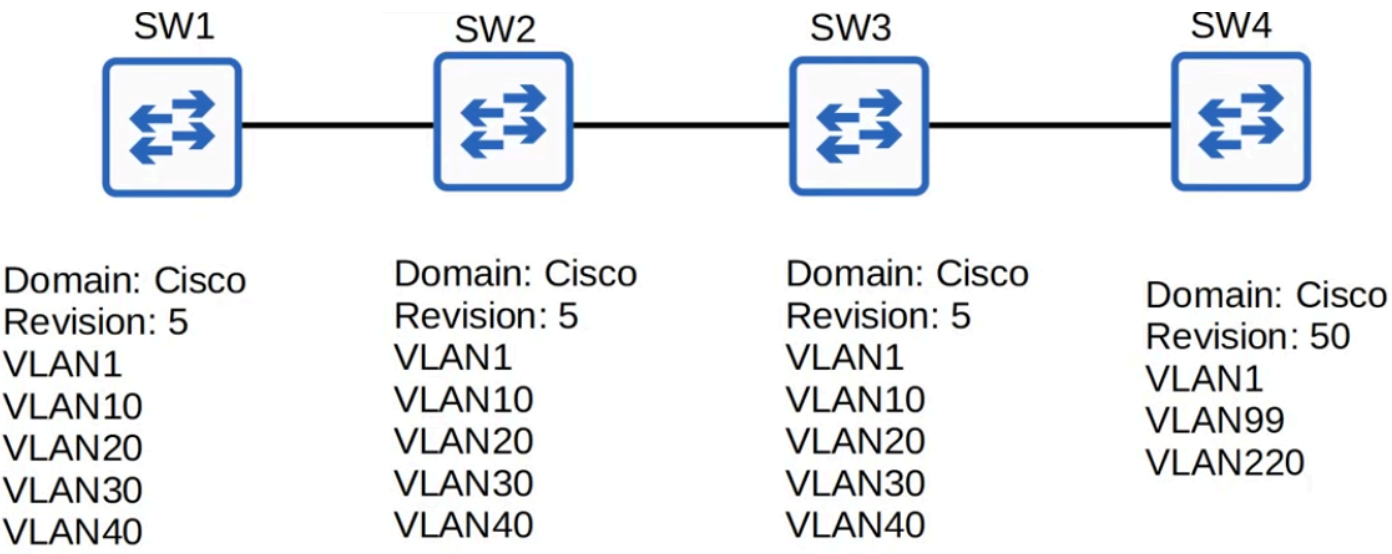


- SW3 and SW4 also **join the domain** `cisco`

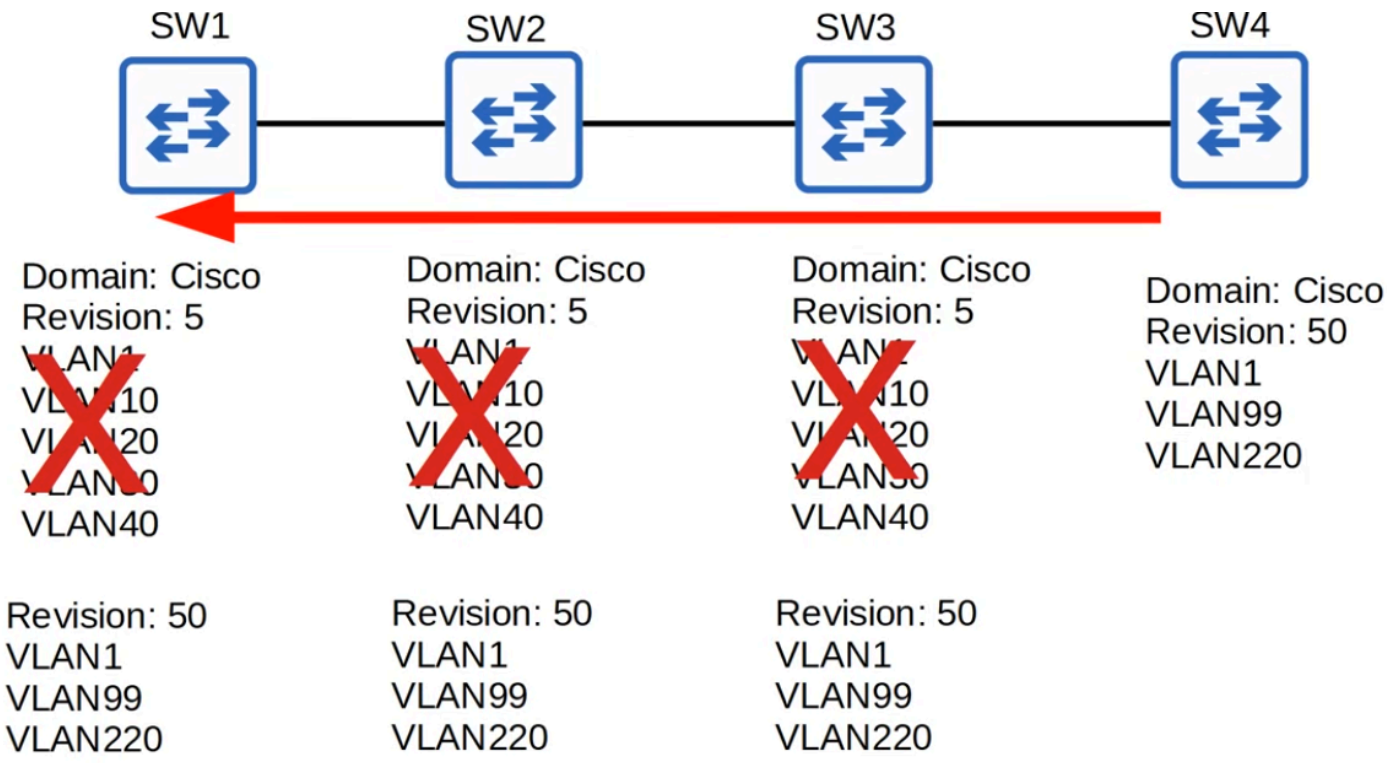
- They **update their VLAN database** to match SW1

The Danger of VTP

Scenario



Switch	Revision Number	VLANs
Current network (domain `cisco`)	5	1, 10, 20, 30, 40
Old switch added to network	**50**	1, 99, 220



What Happens

1. The old switch is connected to the network
2. It sends VTP advertisements with revision number **50**
3. The advertisements are **forwarded throughout the domain**
4. **All switches** update their VLAN database to match the old switch
5. VLANs 10, 20, 30, and 40 **disappear**
6. All hosts in those VLANs **instantly lose connectivity**

Why This is Dangerous

> ***This is one reason why VTP is usually not used in modern networks.***

The entire network's VLAN configuration can be overwritten by a single switch with a higher revision number, causing widespread connectivity loss.

Key Takeaway

- VTP servers also function as **VTP clients** — they will update their own VLAN database if they receive an advertisement with a higher revision number

- Always **reset the revision number to 0** before adding a switch to an existing VTP domain (change domain to an unused name, or change to transparent mode)

Study Notes: VTP Transparent Mode, Client Mode, and VTP Versions

VTP Transparent Mode

Key Characteristics

- **Does not participate** in the VTP domain
- **Does not sync** its VLAN database to the VTP server
- **Maintains its own independent VLAN database** in NVRAM
- **Can add, modify, or delete VLANs** locally, but these changes are **not advertised** to other switches
- **Forwards VTP advertisements** over its trunk ports **only if** the advertisement is in the **same VTP domain** as the transparent switch
- **Will not advertise** its own VLAN database

CLI Command

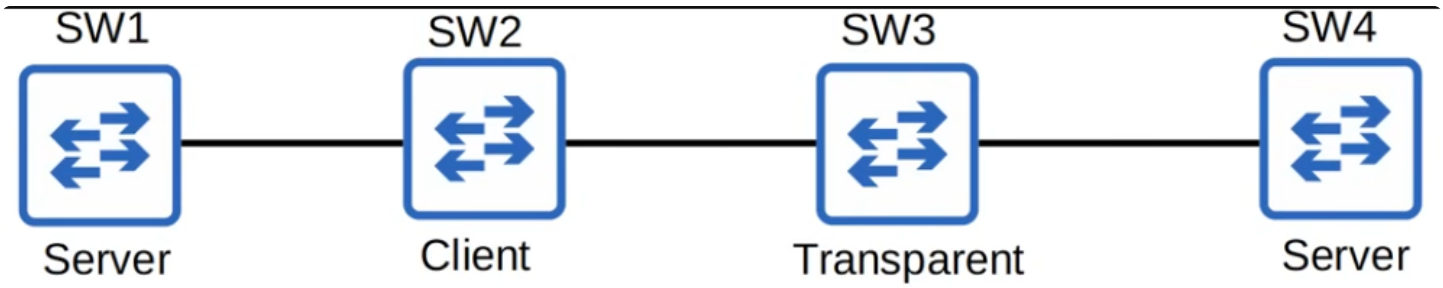
```
vtp mode transparent
```

Comparison of VTP Modes

Feature	VTP Server	VTP Client	VTP Transparent
Add/Modify/Delete VLANs	Yes	No	Yes (locally only)
Store in NVRAM	Yes	No (except VTPv3)	Yes
Respond to VTP advertisements	Yes (synchronizes to higher revision number)	Yes (synchronizes to server)	No (does not sync)
Forward VTP advertisements	Yes	Yes	Yes (only if same domain)

Network Setup for Transparent

Four switches (SW1, SW2, SW3, SW4) are connected.



Lab Demonstration: Client and Transparent Mode

Step 1: Set SW2 to Client Mode

Command:

```
vtp mode client
```

```
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)#
```

Result: Attempting to create VLAN 20 on SW2 is **rejected** because client mode cannot add, modify, or delete VLANs.

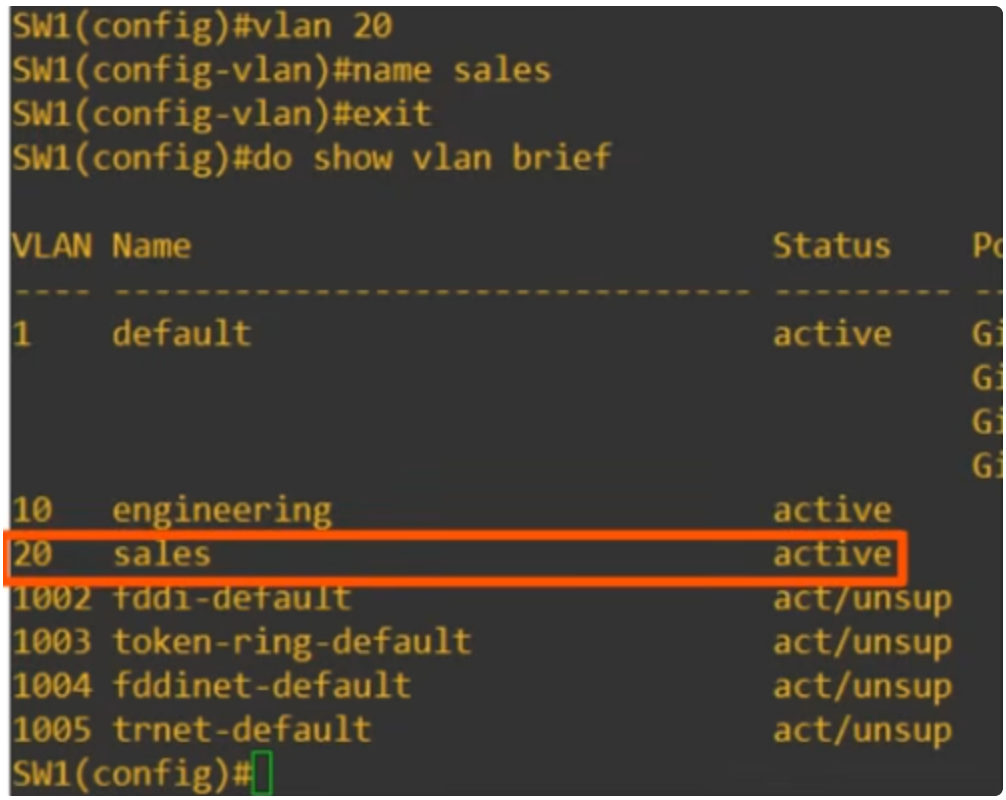
Step 2: Set SW3 to Transparent Mode (Different Domain)

Commands:

```
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)#
```

```
vtp mode transparent
vtp domain juniper
```

Step 3: Create VLAN 20 on SW1



Commands:

```
vlan 20
name sales
```

SW1 `show vtp status`:

```
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
```

- Configuration Revision: **4**
- VLAN 20 appears in `show vlan brief`

Step 4: Check SW2 (Client)

Result:

```
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#
```

- VLAN 20 has been **added** to SW2's VLAN database
- Revision number: **4** (matches SW1)

Step 5: Check SW3 (Transparent, Domain `juniper`)

Result:

```
SW3#show vlan brief

VLAN Name                                Status    P
---- ----------------------------------- --------- -
1    default                             active    G
                                                   G
                                                   G
                                                   G
10   engineering                         active
1002 fddi-default                        act/unsup
1003 token-ring-default                  act/unsup
1004 fddinet-default                     act/unsup
1005 trnet-default                       act/unsup
SW3#
```

```
SW3#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : juniper
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0c09.f9fa.e700
Configuration last modified by 0.0.0.0 at 5-4-20 03:33:08

Feature VLAN:
--------------
VTP Operating Mode              : Transparent
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 6
Configuration Revision          : 0
MD5 digest                      : 0xDB 0x6A 0xDB 0x61 0x
                                  0x59 0x73 0x4E 0xF4 0x

SW3#
```

- VLAN 20 is **NOT added** to SW3's VLAN database
- Revision number: **0** (changing VTP domain or mode to transparent resets revision to 0)

Step 6: Check SW4 (Domain `cisco`)

Result:

```
SW4#show vlan brief

VLAN Name                                Status    P
---- ----------------------------------- --------- -
1    default                             active    G
                                                   G
                                                   G
                                                   G
10   engineering                         active
1002 fddi-default                        act/unsup
1003 token-ring-default                  act/unsup
1004 fddinet-default                     act/unsup
1005 trnet-default                       act/unsup
SW4#
```

```
SW4#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.f972.8700
Configuration last modified by 0.0.0.0 at 5-4-20 03:33:08
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        : 6
Configuration Revision          : 3
MD5 digest                      : 0xFC 0x05 0xC0 0x82 0
```

- VLAN 20 is **NOT present**
- Revision number: **3** (unchanged)

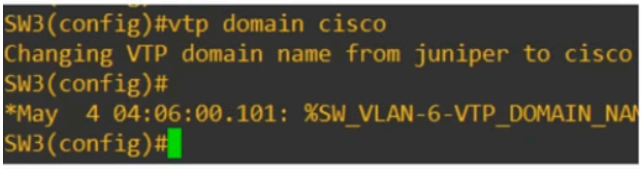
Why? SW3 is in a different domain (`juniper`), so it does **not forward** VTP advertisements to SW4.

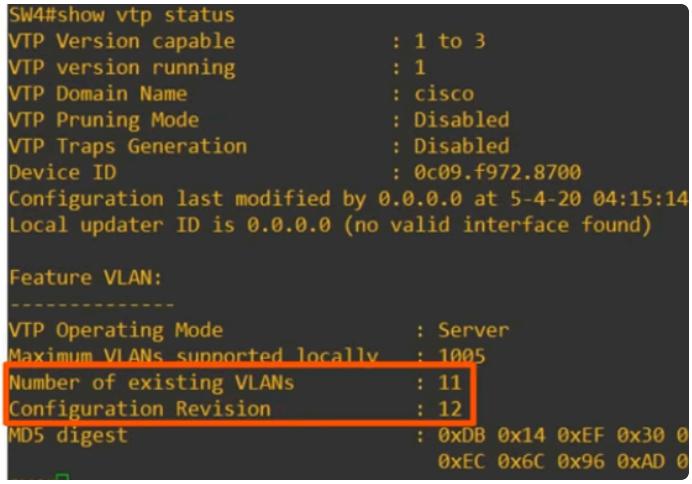
Step 7: Fix Forwarding — Change SW3 Back to Domain `cisco`

Command:

```
vtp domain cisco
```

Result:





- SW3 now **forwards** VTP advertisements to SW4
- SW4 **syncs** its VLAN database to match SW1 and SW2
- SW3 itself still does **not sync** its own VLAN database

Resetting VTP Revision Number to 0

Two common methods:

1. **Change the VTP domain to an unused domain name:**

   ```
   vtp domain [unused-domain-name]
   ```

2. **Change the switch to VTP transparent mode:**

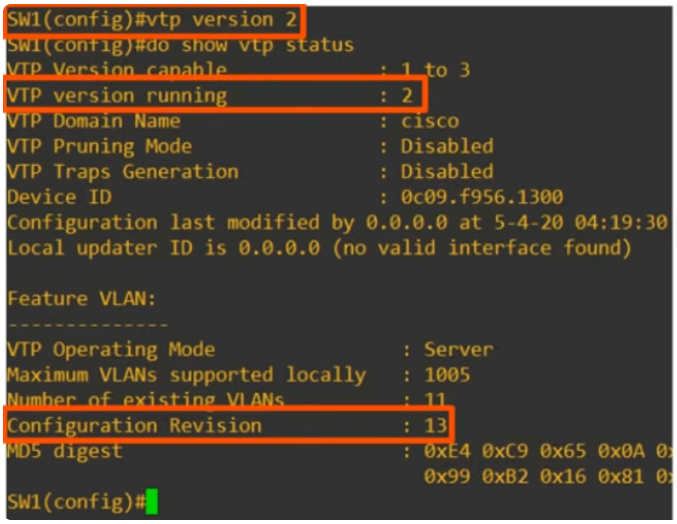
```
vtp mode transparent
```

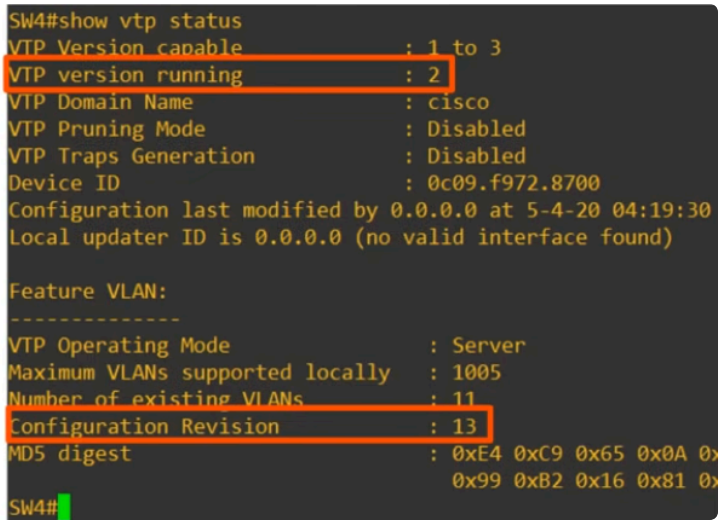
Both reset the revision number to **0**, which is recommended **before** adding a used switch into a VTP domain.

VTP Versions

Changing VTP Version

Command:






```
vtp version [1 | 2 | 3]
```

Important: Changing the VTP version **increases the revision number**, and advertisements with the new revision number are sent. Other servers and clients will sync and start operating in the new version.

Version Differences

Version	Key Features
Version 1	Default on many switches
Version 2	Adds support for **Token Ring VLANs** (not much different from v1 otherwise)
Version 3	Adds support for **extended VLAN range (1006–4094)** and other features beyond CCNA scope

Cisco's Quote on VTP v2

> ***"VTP V2 is not much different than VTP V1. The major difference is that VTP V2 introduces support for Token Ring VLANs. If you use Token Ring VLANs, you must enable VTP V2. Otherwise, there is no reason to use VTP V2."***

Token Ring is an old technology, so there is generally **no reason to use version 2** in modern networks.

Note: Both DTP and VTP were removed from the CCNA 200-301 exam topics list, but knowledge of their functions and basic operation may still appear on the exam.