DTP - Dynamic Trunking Protool
&
VTP - VLAN Trunking Protocol

SDC CNW (CSE 4541)

CSE, FET, ITER
SOA University, BBSR-30

References

Glen E. Clarke & Richard Deal

CCT/CCNA

Routing & Switching Exam Guide

McGrawHll

Todd Lammle

CCNA

Routing & Switching Study Guide

SYBEX, A Wiley Brand

Discussion Flow

- Introduction
- DTP
- Swicth Port Mode
- Trunking Encapsulation
- Exercise on DTP
- VTP & VTP Modes
- Exercise on VTP

Review Questions

Introduction

- DTP and VTP are Cisco proprietary protocols. Both work on Layer 2 of the network reference models.
- DTP is used for the purpose of negotiating trunking on a link between two VLAN-aware switches, and for negotiating the type of trunking encapsulation to be used.
- VLAN trunks formed using DTP may utilize either IEEE 802.1Q or Cisco ISL trunking protocols.
- DTP should not be confused with VTP, as they serve different purposes.
- VTP communicates VLAN existence information between switches.
- VTP propagates the definition of Virtual Local Area Networks (VLAN) on the whole local area network.
- There are three versions of VTP, namely version 1, version 2, version 3.

DTP - Dynamic Trunking Protocol

- DTP is a proprietary Layer 2 protocol designed by Cisco.
- It allows Cisco switches to dynamically determine their interface status (**access** or **trunk**) without manual configuration.
- It is enabled by default on all Cisco switch interfaces.
- Generally, we have been manually configuring switch ports using the commands: `swictport mode access` or `switchport mode trunk`
- For security purposes, manual configuration is recommended. DTP should be disabled on all switches.
- DTP is used for negotiating trunking on a link between two devices as well as negotiating the encapsulation type of either 802.1q or ISL.

Switch port modes

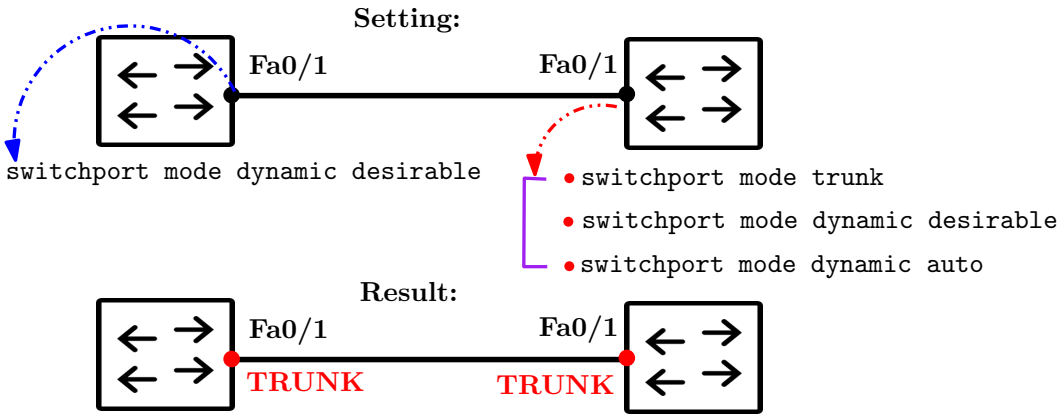
```
SW(config-if)#switchport mode ?
SW(config-if)#switchport mode dynamic ?
```

The following switch port mode settings exist:

- **Access** - Puts the Ethernet port into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The Ethernet port becomes a nontrunk port even if the neighboring port does not agree to the change.
- **Trunk** - Puts the Ethernet port into permanent trunking mode and negotiates to convert the link into a trunk link. The port becomes a trunk port even if the neighboring port does not agree to the change.
- **Dynamic Auto** - Makes the Ethernet port willing to convert the link to a trunk link. The port becomes a trunk port if the neighboring port is set to trunk or dynamic desirable mode. This is the default mode for some switchports.
- **Dynamic Desirable** - Makes the port actively attempt to convert the link to a trunk link. The port becomes a trunk port if the neighboring Ethernet port is set to trunk, dynamic desirable or dynamic auto mode.
- **No-negotiate** - Disables DTP. The port will not send out DTP frames or be affected by any incoming DTP frames. If you want to set a trunk between two switches when DTP is disabled, you must manually configure trunking using the (**`switchport mode trunk`**) command on both sides.

switchport mode Setting

DTP negotiations



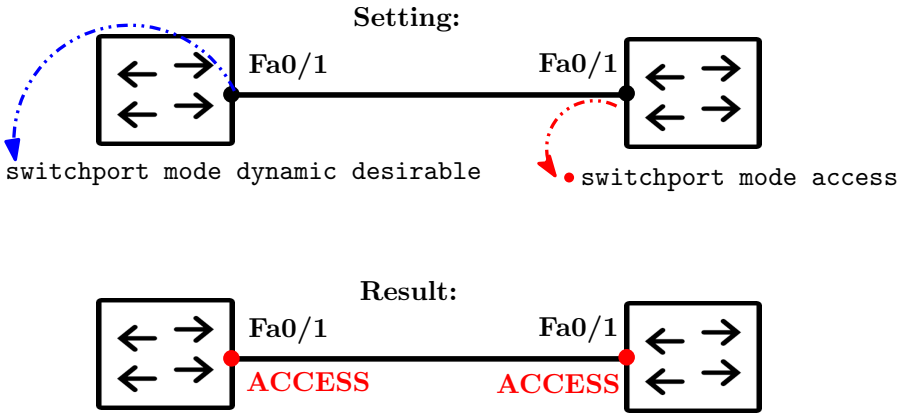
mode: dynamic desirable

A switchport in **dynamic desirable** mode will actively try to form a trunk with other Cisco switches.

Verification command:

```
SW#show int fa0/1 switchport
```

DTP negotiations



mode: dynamic desirable

The right side switch interface is manually configured as **access**

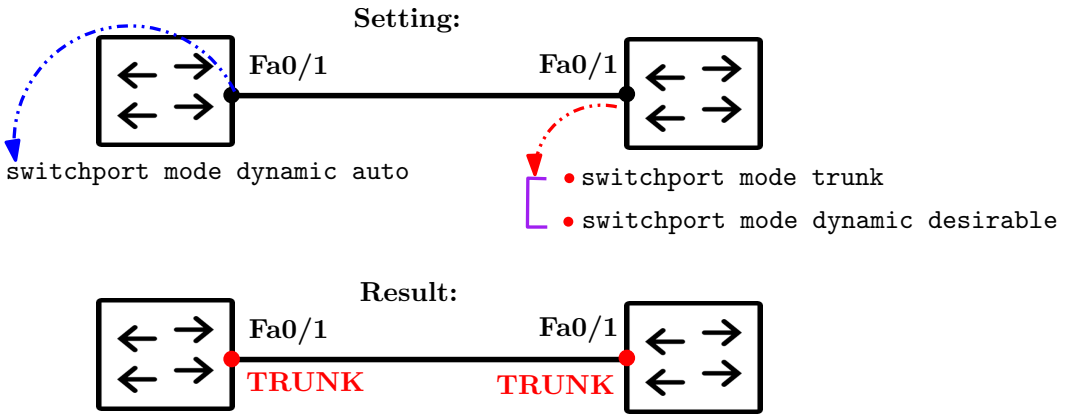
Verification command:

```
SW#show int fa0/1 switchport
```

Static access: It means an access port that belongs to a single VLAN that doesn't change (unless we configure a different VLAN). There are also **dynamic access** ports in which a server automatically assigns the VLAN depending on the MAC address of the connected device.

switchport mode Setting Contd...

DTP negotiations



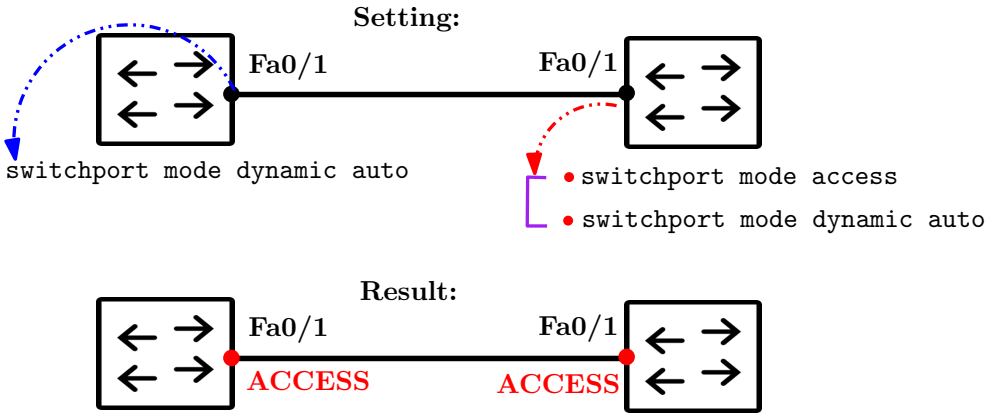
mode: dynamic auto

A switchport in **dynamic auto** mode will NOT actively try to form a trunk with other Cisco switches.

Verification command:

```
SW#show int fa0/1 switchport
```

DTP negotiations



mode: dynamic auto

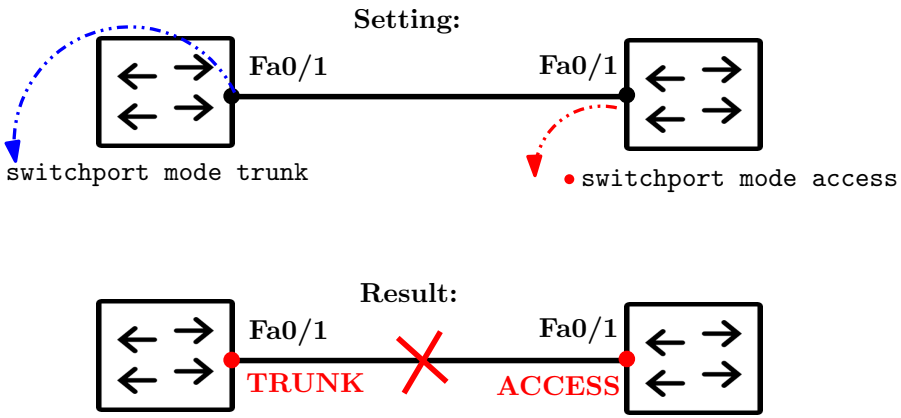
The right side switch interface is manually configured as **access** and as well **dynamic auto**

Verification command:

```
SW#show int fa0/1 switchport
```

switchport mode Setting Contd...

DTP negotiations



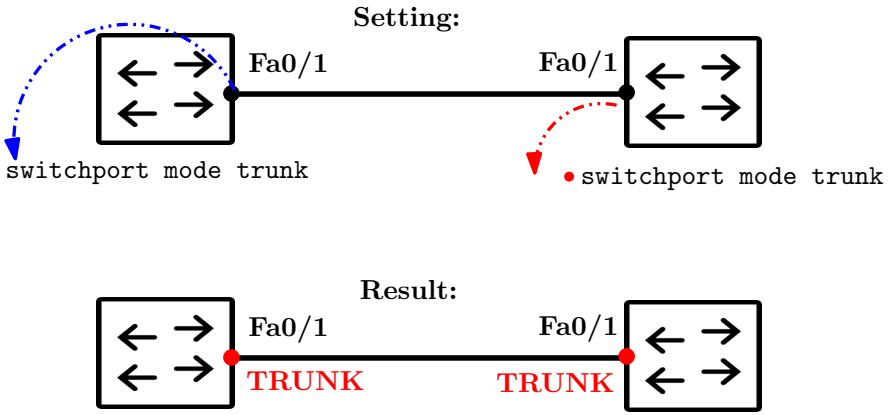
mode: access

A switchport in **dynamic desirable** mode will actively try to form a trunk with other Cisco switches.

Verification command:

```
SW#show int fa0/1 switchport
```

DTP negotiations



mode: trunk

The right side switch interface is manually configured as **trunk**

Verification command:

```
SW#show int fa0/1 switchport
```

If both side switchport mode manually configured as **ACCESS**, then switch interface will be in ACCESS.

Sumary: Switchport mode

Administrative Mode	Trunk	Dynamic Desirable	Access	Dynamic Auto
Dynamic Auto	Trunk	Trunk	Access	Access
Dynamic Desirable	Trunk	Trunk	Access	Trunk
Trunk	Trunk	Trunk	✖	Trunk
Access	✖	Access	Access	Access

NOTE: DTP will not form a trunk with a router, PC etc. The switchport will be in access mode.

DTP Conclusive Points

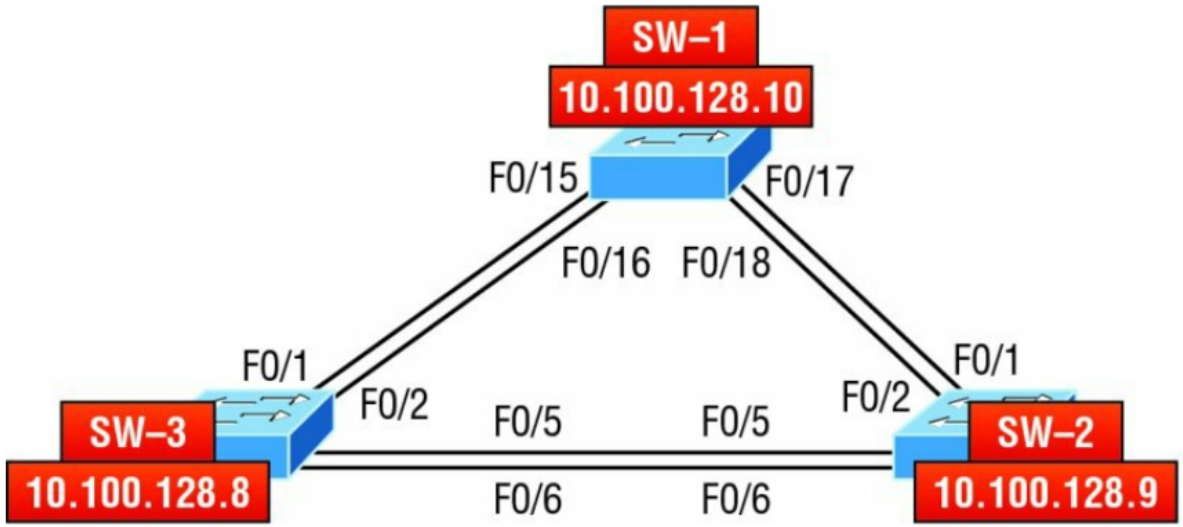
- In older switches, **`switchport mode dynamic desirable`** is the default administrative mode.
- In newer switches, **`switchport mode dynamic auto`** is the default administrative mode.
- We can disable DTP negotiation with **`switchport nonegotiate`** command on an interface.
- Configuring an access port with **`switchport mode access`** also disables DTP negotiation on an interface.
- It is recommended that DTP to be disabled on all switchports and manually configure them as access or trunk ports for security reasons.

Trunking Encapsulation

- Switches that support both 802.1Q and ISL trunk encapsulation can use DTP to negotiate the encapsulation they will use.
- The negotiation is enabled by default, as the default trunk encapsulation mode is
  `switchport trunk encapsulation negotiate`
- We can disable DTP negotiation with **`switchport nonegotiate`** command on an interface.
- ISL is favored over 802.1Q, so if both switches support ISL it will be selected.
- DTP frames are sent in VLAN 1 when using ISL, or in the native VLAN when using 802.1Q (the default native VLAN is VLAN 1, however).

Exercise on DTP

Check switchport mode of the given configuration



DTP verification (Check supports for CPT)

- Check the switch port modes of the switches
- Change any switchport mode to truck, and verify others
- Change any switchport mode to access, and verify others
- Change any switchport mode to dynamic auto, and verify others
- Change any switchport mode to dynamic desirable, and verify others

VTP
VLAN Trunking Protocol

VTP - Introduction

- VLAN Trunking Protocol (VTP) is a Cisco proprietary Layer-2 protocol.
- The basic goals of VTP are to manage all configured VLANs across a switched internetwork and to maintain consistency throughout that network.
- VTP allows you to add, delete, and rename VLANs information that is then propagated to all other switches in the VTP domain.
- VTP carries VLAN information to all the switches in a VTP domain.
- VTP advertisements can be sent over 802.1Q, and ISL trunks.
- Three versions of VTP: version 1, 2, and 3.
- VTP allows to configure VLANs on a central VTP server switch and other switches (VTP clients) will synchronize their VLAN database to the server.

VTP Benefits

- Consistent VLAN configuration across all switches in the network.
- Dynamic reporting of added VLANs to all switches in the VTP domain.
- Accurate tracking and monitoring of VLANs.
- Adding VLANs using Plug and Play
- VLAN trunking over mixed networks, such as Ethernet to ATM LANE or even FDDI.

How Does VTP Work to manage VLANs across the network ?

- Three VTP modes: **Server**, **Client** and **transparent**.
- Cisco switches operate in VTP server mode by default.
- All servers that need to share VLAN information must use the **same domain name** and **password**.
- A switch can be in only one domain at a time.
- VTP information is sent between switches only via a trunk port.
- Switches advertise VTP management domain information as well as a configuration revision number and all known VLANs with any specific parameters.
- **VTP transparent mode:** Switches are configured to forward VTP information through trunk ports but not to accept information updates or update their VLAN databases.

VTP modes: Server, Client, and Transparent

1. VTP Server

- It can add/modify/delete VLANs.
- It stores the VLAN database in non-volatile RAM(NVRAM)
- It will increase the **revision number** every time a VLAN is added/modified/deleted.
- It will advertise the latest version of the VLAN databse on trunk interfaces, and the VTP client will synchronize their VLAN database to it.
- VTP server also function as VTP clients. Therefore a VTP server will synchronize to another VTP server with a higher revision number.

2. VTP Client

- Cannot add/modify/delete VLANs.
- Do not store the VLAN database in non-volatile RAM(NVRAM)
- Will synchronize their VLAN database to the server with the highest revision number in their VTP domain
- Will advertise their VLAN database and forward VTP advertisements to other clients over their trunk ports.

VTP modes: Contd...

3. VTP Transparent

- Does not participate in the VTP domain or share its VLAN database.
- Maintains its own database in NVRAM. It can add/modify/delete VLANs of own, but they won't be advertised to other switches.
- Will forward VTP advertisements that are in the same domain as it.
- Switches in VTP transparent mode advertise VTP management domain information as well as a configuration revision number and all known VLANs with any specific parameters.
- The whole purpose of transparent mode is to allow remote switches to receive the VLAN database from a VTP Server configured switch through a switch that is not participating in the same VLAN assignments.

VTP related Commands

- `SW1#config t`
- `SW1(config)#vtp ?`

```
domain          Set the name of the VTP administrative domain
mode            Configure VTP device mode
password        Set the password for the VTP administrative domain
Version         Set the administrative domain to VTP version
```

- `SW1(config)#vtp mode ?`

```
client          Set the device to client mode
server          Set the device to server mode
transparent     Set the device to transparent mode
```

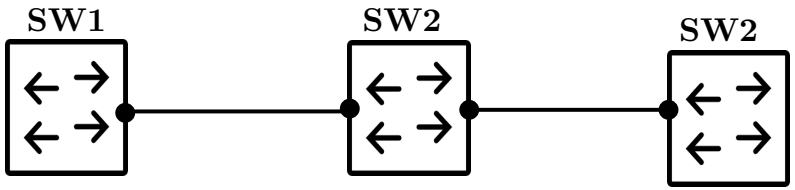
- `SW1(config)#vtp domain ITER` /* ITER - VTP domain name */

```
SW1#config t
SW1(config)#vtp domain ITER
VTP Version capable                 : 1 to 2
VTP Version running                 : 1
VTP Domain Name                     :  ITER
VTP Pruning Mode                    : Disabled
::::::::
```

A Simple Case with VTP

Observe a Case with VTP by default

All the interfaces are configired as Trunk



Run the command on any switch

`SW1#show vtp status`

All the switches are in default VTP configuration, So output will be same.

```
SW1#show vtp status
VTP Version capable                 : 1 to 2
VTP Version running                 : 1
VTP Domain Name                     :
VTP Pruning Mode                    : Disabled
Device ID                           : 0090.0C14.CD00
Configuration last modeified by 0.0.0.0 at 0-0-0 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN :
--------------------
VTP Operation  Mode                 : Server
Maximum VLANS supported locally     : 255
Number of existing VLANS            : 5
Configuration Revision              : 0
MD5 digest                          : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
                                      0xF0 0x58 0x10 0x6C 0x9C 0x0F 0xA0 0xF7
SW1#
```

VTP Domain Name

Create a VTP domain on SW1 as **ITER**. Also create a VLAN 10 on SW1 and once again check the VTP status.

```
SW1(config)#vtp domain ITER
SW1(config)#vlan 10
SW1(config-vlan)#name CSEngg
SW1(config-vlan)#exit
```

```
SW1#show vtp status
VTP Version capable             : 1 to 2
VTP Version running             : 1
VTP Domain Name                 :  ITER
VTP Pruning Mode                : Disabled
Device ID                       : 0090.0C14.CD00
Configuration last modeified by 0.0.0.0 at 0-0-0 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN :
--------------------
VTP Operation  Mode              : Server
Maximum VLANS supported locally  : 255
Number of existing VLANS        : 6
Configuration Revision          :  1
MD5 digest                      : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
                                  0xF0 0x58 0x10 0x6C 0x9C 0x0F 0xA0 0xF7
SW1#
```

VTP SW2 and SW3

- 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 it's VLAN database to match.
- **Testing:** `SW2#show vtp status`, `SW2(config)#show vlan brief`

```
SW2#show vtp status
VTP Version capable             : 1 to 2
VTP Version running             : 1
VTP Domain Name                 :  ITER
::::::::::::::::::

Feature VLAN :
--------------------
VTP Operation  Mode              : Server
Maximum VLANS supported locally  : 255
Number of existing VLANS         : 6
Configuration Revision           :  1
::::::::::::
SW2#
```

```
SW2#show vlan brief
VLAN Name
--------------------------
1 default

10     CSEngg
1002   fddi-default
1003   token-ring-default
1004   fddinet-default
1005   trnet-default
SW2#
```

- **Testing:** `SW3#show vtp status`, `SW3(config)#show vlan brief`
- **Observations:** Switch SW2 and SW3 join the VTP domain and update their VLAN databases.

Danger with VTP

If you connect an old switch with a higher revision number to your network (and the VTP domain name matches), all switches in the domain will sync their VLAN database to that switch.

Reason:

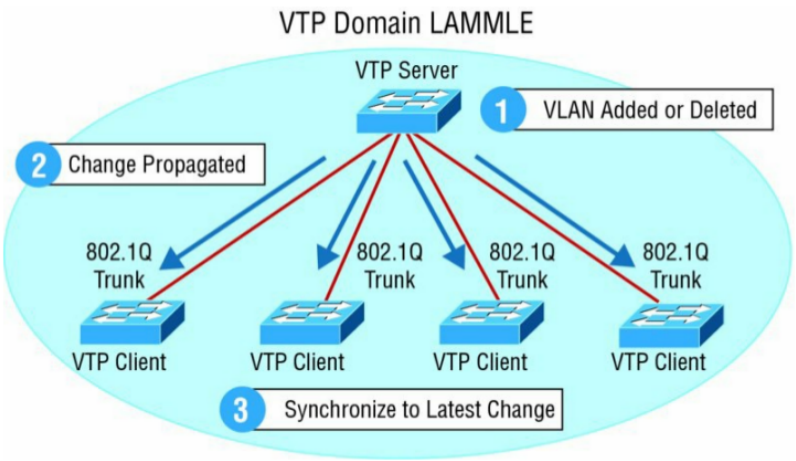
- Switches detect any added VLANs within a VTP advertisement and then prepare to send information on their trunk ports with the newly defined VLAN.
- Updates are sent out as revision numbers that consist of summary advertisements.
- Anytime a switch sees a higher revision number, it knows the information it's getting is more current, so it will overwrite the existing VLAN database with the latest information.

Requirements for VTP to communicate VLAN information between switches:

- The VTP version must be set the same
- The VTP management domain name of the switches must be set the same.
- One of the switches has to be configured as a VTP server.
- Set a VTP password if used.

Summary: VTP Modes of Operation

VTP Modes



- **Server** is the default mode for all Catalyst switches.
- At least one server is needed in VTP domain to propagate VLAN information throughout that domain.
- The switch must be in server mode to be able to create, add, and delete VLANs in a VTP domain.
- VLAN information has to be changed in server mode, and any change made to VLANs on a switch in server mode will be advertised to the entire VTP domain.
- Figure shows how a VTP server will update the connected VTP client's VLAN database when a change occurs in the VLAN database on the server.

- **Client:** In client mode, switches receive information from VTP servers. Clients receive and forward updates, so in this way, they behave like VTP servers.
- Client can not create, change, or delete VLANs. Additionally, none of the ports on a client switch can be added to a new VLAN before the VTP server notifies the client switch of the new VLAN and the VLAN exists in the client's VLAN database.
- VLAN information sent from a VTP server isn't stored in NVRAM of the client. It means that if the switch is reset or reloaded, the VLAN information will be deleted.
- So basically, a switch in VTP client mode will forward VTP summary advertisements and process them. This switch will learn about but won't save the VTP configuration in the running configuration, and it won't save it in NVRAM. Switches that are in VTP client mode will only learn about and pass along VTP information.

NOTE: VTP

- VTP only learns about normal-range VLANs, with VLAN IDs 1 to 1005.
- VLANs with IDs greater than 1005 are called extended-range VLANs and they're not stored in the VLAN database.
- The switch must be in VTP transparent mode when you create VLAN IDs from 1006 to 4094.
- Switches in transparent mode don't participate in the VTP domain or share its VLAN database, but they'll still forward VTP advertisements through any configured trunk links. They can create, modify, and delete VLANs because they keep their own database-one they keep secret from the other switches.
- The whole purpose of transparent mode is to allow remote switches to receive the VLAN database from a VTP Server configured switch through a switch that is not participating in the same VLAN assignments.
- VLAN database in transparent mode is actually only locally significant.
- VLAN IDs 1 and 1002 to 1005 are automatically created on all switches and cant be removed.

Configuring VTP

- All Cisco switches are configured to be VTP servers by default.
- To configure VTP: (i) configure the domain name (ii) set the VTP version, domain name, password, operating mode, and pruning capabilities of the switch (iii) verify vtp.

```
S1#config t
S1#(config)#vtp mode server
Device mode already VTP SERVER.
S1(config)#vtp domain Lammle
Changing VTP domain name from null to Lammle
S1(config)#vtp password todd
Setting device VLAN database password to todd
S1(config)#do show vtp password
VTP Password: todd

S1(config)#do show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        :8
VTP Operating Mode              : Server
VTP Domain Name                 : Lammle
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest: 0x15 0x54 0x88 0xF2 0x50 0xD9 0x03 0x07
Configuration last modified by 192.168.24.6 at 3-14-93 15:47:32
Local updater ID is 192.168.24.6 on interface Vl1 (lowest numbered VLAN
      interface found)
```

VTP Pruning

- VTP gives you a way to preserve bandwidth by configuring it to reduce the amount of broadcasts, multicasts, and unicast packets. This is called pruning.
- Switches enabled for VTP pruning send broadcasts only to trunk links that actually must have the information.
- **Example:** If Switch A doesn't have any ports configured for VLAN 5 and a broadcast is sent throughout VLAN 5, that broadcast wouldn't traverse the trunk link to Switch A.
- By default, VTP pruning is disabled on all switches.
- When you enable pruning on a VTP server, you enable it for the entire domain.
- By default, VLANs 2 through 1001 are pruning eligible, but VLAN 1 can never be pruned because it's an administrative VLAN.
- VTP pruning is supported with both VTP version 1 and version 2.

VTP Pruning:

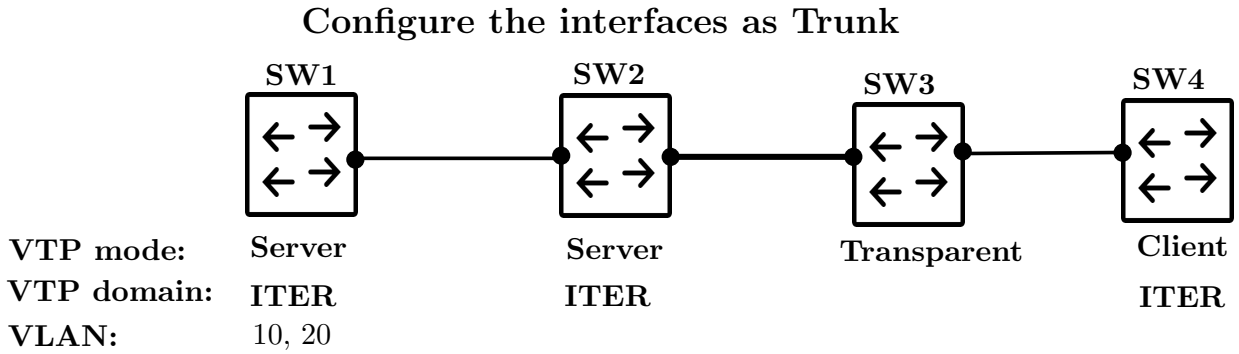
- `S1#sh int trunk` Shows all VLANs that are allowed across a trunked link by default.
- Check the output of the above command for VTP pruning is disabled by default.
- **Enable pruning:** takes one command and it is enabled on entire switched network for the listed VLANs.

```
S1#config t
S1(config)#int f0/1
S1(config-if)#switchport trunk ?
S1(config-if)#switchport trunk pruning ?
S1(config-if)#switchport trunk pruning vlan 3-4
```

- The valid VLANs that can be pruned are 2 to 1001. Extended-range VLANs (VLAN IDs 1006 to 4094) can't be pruned, and these pruning-ineligible VLANs can receive a flood of traffic.

Exercise on VTP

VTP Configuration & Verification



- Configure the above switched netwrok and check the `vtp status` at switch **SW1**.
- Verify the VTP status at other switches and draw the conclusion.
- Now, Change the VTP domain name, CSE, at Switch SW2 and create a new VLAN at switch SW1.
- Verify the VTP status at switch SW2. Conclude whether SW2 receives the update VTP revision number from SW1 or not. Justify the reason
- Verify the VTP status at switch SW3 and draw the conclusion.
- Try to create a VLAN at switch SW4 and draw the conclusion. Find a way to create VLAN at SW4.

Troubleshooting VTP

Guidelines:

- Check & verify the output on switches: **`Switch#sh vtp status`**
- Switches in VTP server mode will share VLAN information. For that VTP domain names should be configured same over the switches.
- If all switches can be servers and they can still share VLAN information.
- If the VTP mode is client for any switch, then a VTP client cannot create, delete, or change VLANs,
- VTP clients only keep the VTP database in RAM, and that's not saved to NVRAM.
- To create a VLAN on a switch (VTP mode is client), it is required to make that switch in VTP server first.
- VTP VLAN information with the highest revision number can be only receive on switches.
- By default, VTP operates in version 1.
- You can configure VTP version 2 if you want support for these features, which are not supported in version 1:
  - Token Ring support
  - Unrecognized Type-Length-Value (TLV) support
  - Version-Dependent Transparent Mode
  - Consistency Checks

Review Questions

1. Which is not a mode in VTP?

   (A) DHCP
   (B) Client
   (C) Server
   (D) Transparent

2. By default switches are in which VTP mode.

   (A) Server
   (B) Client
   (C) Transparent
   (D) All modes

3. VLAN database in VTP server mode stores in.

   (A) NVRAM
   (B) RAM
   (C) ROM
   (D) HDD

4. VLAN database in VTP client mode stores in.

   (A) NVRAM
   (B) RAM
   (C) ROM
   (D) HDD

THANK YOU