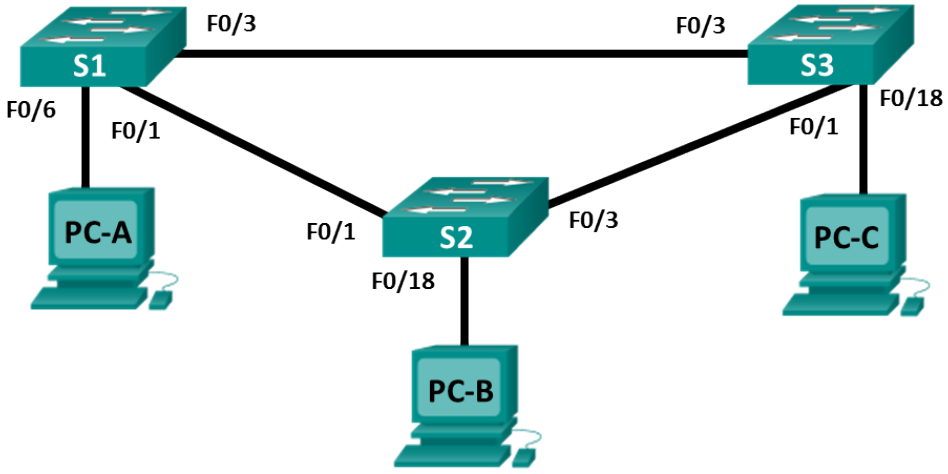
Shaun Lim
Aldrich Go
Amienz Arago
Dave Bolima

Lab 4.1 – Configure Extended VLANs, VTP, and DTP

Topology



Addressing Table

Table Heading	Interface	IP Address	Subnet Mask
S1	VLAN 99	192.168.99.1	255.255.255.0
S2	VLAN 99	192.168.99.2	255.255.255.0
S3	VLAN 99	192.168.99.3	255.255.255.0
PC-A	NIC	192.168.10.1	255.255.255.0
PC-B	NIC	192.168.20.1	255.255.255.0
PC-C	NIC	192.168.10.2	255.255.255.0

Objectives

Part 1: Configure Dynamic Trunking Protocol

Part 2: Configure VLAN Trubnking Protocol

Part 3: Add VLANs and Assign Ports

Part 4: Configure Extended VLAN

Background / Scenario

It can become challenging to manage VLANs and trunks in a network as the number of switches increases. VLAN trunking protocol (VTP) allows a network administrator to automate the management of VLANs. Automated trunk negotiation between network devices is managed by the Dynamic Trunking Protocol (DTP). DTP is enabled by default on Catalyst 2960 and Catalyst 3560 switches.

In this lab, you will configure trunk links between the switches. You will also configure a VTP server and VTP clients in the same VTP domain. Furthermore, you will configure an extended VLAN on one of the switches, assign ports to VLANs and verify end-to-end connectivity within the same VLAN.

Required Resources

- 3 Switches (Cisco 2960)
- 3 PCs
- Ethernet cables as shown in the topology

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings on the PC hosts and switches.

Step 1: Cable the network as shown in the topology.

Attach the devices as shown in the topology diagram, and cable as necessary.

Step 2: Step 2: Configure basic settings for each switch.

a. Console into the switches and enable privileged EXEC mode.

b. Open configuration window

c. Enter configuration mode.

d. Assign device names to the switches.

Part 2: Configure DTP

In Part 2, you will configure interface F0/1 of S1 and S2 to use the Dynamic Trunking Protocol (DTP) to allow it to negotiate a trunk link between the switches. You will also configure a static trunk link between S1 and S3.

Step 1: Configure dynamic trunk links between S1 and S2.

The default DTP mode of a 2960 switch port is dynamic auto. This allows the interface to convert the link to a trunk if the neighboring interface is set to trunk or dynamic desirable mode.

a. Enter the **show interfaces f0/1 switchport** command on S1 and S2.

What is the administrative and operational mode of switchport f0/1?

Switch	Operational Mode	Administrative Mode
S1	Static access	Dynamic auto
S2	Static access	Dynamic auto

b. In interface configuration mode, configure a dynamic trunk link between S1 and S2. Because the default mode is dynamic auto, only one side of the link needs to be configured as dynamic desirable.

```
S1(config)# interface f0/1
S1(config-if)# switchport mode dynamic desirable
S1(config-if)#
*Mar  1 00:30:45.082: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down
*Mar  1 00:30:48.102: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
```

c. Verify trunking link between S1 and S2 using the **show interfaces trunk** command.

```
S1# show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       desirable        802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       none
```

```
S2# show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       auto             802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1
```

d. Enter the **show interfaces f0/1 switchport** command again on S1 and S2.

What are the administrative and operational modes of switchport f0/1 on the switches?

Switch	Operational Mode	Administrative Mode
S1	Trunk	Dynamic Desirable
S2	Trunk	Dynamic Auto

What is the difference between the operational and administrative mode of a switchport?

The administrative mode indicates what the interface is capable of doing by default while the operational mode indicates its current mode.

Step 2: Configure static trunk link between S1 and S3.

a. Between S1 and S3, configure a static trunk link using the **switchport mode trunk** command in the interface configuration mode for port F0/3.

```
S1(config)# interface f0/3
S1(config-if)# switchport mode trunk
```

b. Verify the trunks using **show interfaces trunk** command on S1.

```
S1# show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       desirable        802.1q         trunking      1
Fa0/3       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-4094
Fa0/3       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1
Fa0/3       1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       none
Fa0/3       none
```

c. Configure a permanent trunk between S2 and S3.

d. Record the commands you used to create the static trunk.

S2

interface f0/3

switchport mode trunk

S3

interface f0/1

switchport mode trunk

Part 3: Configure VTP

All the switches will be configured to use VTP for VLAN updates. S2 will be configured as the server. Switches S1 and S3 will be configured as clients. They will be in the **CCNA** VTP domain using the password **cisco**.

a. Configure S2 as a VTP server in the **CCNA** VTP domain using **cisco** as the VTP password.

```
S2(config)# vtp domain CCNA
Changing VTP domain name from NULL to CCNA
S2(config)#
*Mar  1 00:03:44.193: %SW_VLAN-6-VTP_DOMAIN_NAME_CHG: VTP domain name changed to CCNA.
S2(config)# vtp mode server
Device mode already VTP Server for VLANS.
S2(config)# vtp password cisco
Setting device VTP password to cisco
```

b. Configure S1 and S3 as VTP clients in the **CCNA** VTP domain using **cisco** as the VTP password. VTP configurations are displayed below.

```
S1(config)# vtp domain CCNA
Changing VTP domain name from NULL to CCNA
S1(config)#
*Mar  1 00:03:44.193: %SW_VLAN-6-VTP_DOMAIN_NAME_CHG: VTP domain name changed
to CCNA.
S1(config)# vtp mode client
Device mode VTP client for VLANS.
S1(config)# vtp password cisco
Setting device VTP password to cisco
```

c. Verify VTP configurations by entering the **show vtp status** command on all switches. The VTP status for S2 is displayed below.

```
S2# show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : CCNA
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0cd9.96d2.3580
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00

Feature VLAN:
--------------
VTP Operating Mode              : Server
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
Configuration Revision          : 0
MD5 digest                      : 0x8B 0x58 0x3D 0x9D 0x64 0xBE 0xD5 0xF6
                                  0x62 0xCB 0x4B 0x50 0xE5 0x9C 0x6F 0xF6
```

Part 4: Add VLANs and Assign Ports

Step 1: Add VLANs on the switches.

a. On S1, add VLAN 10.

```
S1(config)# vlan 10
```

Were you able to create VLAN 10 on S1? Why or why not?

No, because s1 is in VTY client mode.

b. On S2, add the following VLANs and examine the VLAN database.

VLAN	Name
10	Red
20	Blue
30	Yellow
99	Management

```
S2(config)# vlan 10
S2(config-vlan)# name Red
S2(config-vlan)# vlan 20
S2(config-vlan)# name Blue
S2(config-vlan)# vlan 30
S2(config-vlan)# name Yellow
S2(config-vlan)# vlan 99
S2(config-vlan)# name Management
S2(config-vlan)# end
S2# show vlan brief
```

Were you able to create VLANs on S2? Why or why not?

Yes, this is because S2 is configured with VTY server.

Step 2: Verify VTP status on S2

Adding VLANs and naming them on S2 updates the VLAN configuration version on the switch. Issue the command **show vtp status** on S2.

What is the current configuration revision number on S2?	1
How many VLANs currently exist on S2?	9

Step 3: Verify VLAN database updates on S1 and S3.

Because S1 and S3 are configured as VTP clients, S1 and S3 should learn and implement the VLAN information from S2. Use the **show vtp status** command on S1 and S3.

What is the current configuration revision number on S1 and S3?	1
How many VLANs currently exist on S1 and S3?	9

What **show** command can you use to verify if S1 and S3 indeed synchronized their VLAN database with the VTP server?

do show vlan brief

Step 4: Assign ports to VLANs.

In this step, you will associate ports to VLANs and configure IP addresses according to the table below.

Port Assignment	VLAN	Attached PC IP Address and Prefix
S1 F0/6	VLAN 10	PC-A: 192.168.10.1 / 24
S2 F0/18	VLAN 20	PC-B: 192.168.20.1 /24
S3 F0/18	VLAN 10	PC-C: 192.168.10.2 /24

a. On S1, configure F0/6 to access mode and assign F0/6 to VLAN 10.

```
S1(config)# interface f0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
```

b. Repeat the procedure for switchport F0/18 on S2 and S3. Assign the VLAN according to the table above.

c. Assign the IP addresses to the PCs according to the table above.

Step 5: Configure IP addresses on the switches.

a. On S1, assign an IP address to the SVI for VLAN 99 according to the Addressing Table and activate the interface.

```
S1(config)# interface vlan 99
S1(config-if)# ip address 192.168.99.1 255.255.255.0
S1(config-fi)# no shutdown
```

b. Repeat step a. for S2 and S3.

Step 6: Verify end-to-end connectivity

Perform connectivity tests between hosts in the network.

Can PC-B ping PC-A?	No, due to different networks
Can PC-C ping PC-A?	Yes

Can S1 ping PC-A?	No, due to different networks
Can S1 ping S2?	Yes

Are these results expected? Why or why not?

Yes, this is because we have now configured VLANS and assigned the aforementioned ip address in their respective VLANS, thus “separating” it into their own network. This means without a router, PC-A and PC-B, S1 and PC-A cannot ping each other since they are in separate VLANS.

Part 5: Configure Extended VLAN

An extended VLAN is a VLAN between 1025 and 4096. Because the extended VLANs cannot be managed with VTP, VTP must be configured in transparent mode. In this part, you will change the VTP mode on S1 to transparent and create an extended VLAN on S1.

Step 1: Configure VTP mode to transparent on S1.

a. On switch S1, set VTP mode to transparent.

```
S1(config)# vtp mode transparent
Setting device to VTP Transparent mode for VLANS.
S1(config)# exit
```

b. Verify the VTP mode on S1.

```
S1# show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : CCNA
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0cd9.96e2.3d00
Configuration last modified by 0.0.0.0 at 3-1-93 02:36:11

Feature VLAN:
--------------
VTP Operating Mode                : Transparent
Maximum VLANs supported locally   : 255
Number of existing VLANs          : 9
Configuration Revision            : 0
MD5 digest                        : 0xB2 0x9A 0x11 0x5B 0xBF 0x2E 0xBF 0xAA
                                    0x31 0x18 0xFF 0x2C 0x5E 0x54 0x0A 0xB7
```

Step 2: Configure an extended VLAN on S1.

a. Display the current VLAN configurations on S1.

b. Create an extended VLAN 2000.

```
S1# conf t
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)# vlan 2000
S1(config-vlan)# end
```

c. Verify the VLAN creation.

```
S1# show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/2, Fa0/4, Fa0/5, Fa0/7
                                                 Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                 Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                 Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                 Fa0/24, Gi0/1, Gi0/2
10   Red                               active    Fa0/6
20   Blue                              active
30   Yellow                            active
99   Management                        active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
2000 VLAN2000                          active
```

Step 3: Verify VLAN databases on S2 and S3

Display the current VLAN configurations on S2 and S3.

Does VLAN 2000 exist on S2 and S3?

No

Given the results, describe how transparent switches behave in terms of VLAN synchronization in a VTP domain.

Transparent switches do not synchronize its VLAN configuration based on received advertisements and does not advertise its VLAN configuration.

Part 6: Delete the VLAN Database and VTP Settings

In Part 6, you will delete the VLAN Database from the switch. This procedure also resets the VTP settings of the switch to default. It is necessary to do this when initializing a switch back to its default settings.

Step 1: Delete the VLAN database.

a. Issue the **delete vlan.dat** command to delete the vlan.dat file from flash and reset the VLAN database back to its default settings. You will be prompted twice to confirm that you want to delete the vlan.dat file. Press Enter both times.

```
S1# delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
```

b. Issue the **show flash** command to verify that the vlan.dat file has been deleted.

```
S1# show flash:
```

c. Issue the **reload** command to reboot the switch and clear all current configurations.

```
S1# reload
System configuration has been modified. Save? [yes/no]:no
Proceed with reload? [confirm]
```

Step 2: Verify that VTP settings have been restored to default

Issue the **show vtp status** command to verify that the VTP settings of the switches have been reset to their default values.

What is the current configuration revision number?	0
What is the VTP domain name?	ccna

Reflection

1. What are the advantages and disadvantages of using VTP?

   The advantage of VTP is ease in configuration, but the disadvantage is the difficulty in customization.

2. Why is it important to ensure a proper reset of VTP settings before a switch is connected to an existing network?

   If you did not reset the VTP, the next time the switch boots up, it has to learn again the VLAN config.

3. What are the advantages of using DTP?

   DTP is dynamic trunk protocol and allows us easier management and auto negotiate if a link will be trunked or accessed.