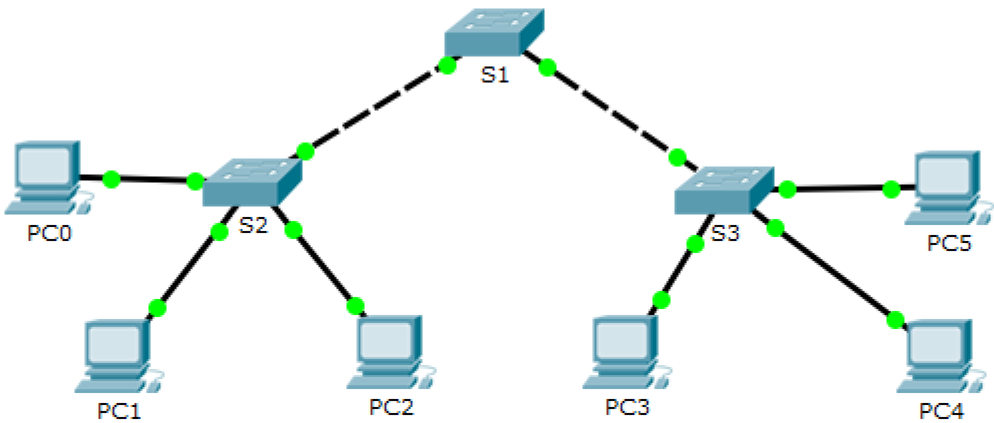
Packet Tracer – Configure VLANs, VTP and DTP

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
PC0	NIC	192.168.10.1	255.255.255.0
PC1	NIC	192.168.20.1	255.255.255.0
PC2	NIC	192.168.30.1	255.255.255.0
PC3	NIC	192.168.30.2	255.255.255.0
PC4	NIC	192.168.20.2	255.255.255.0
PC5	NIC	192.168.10.2	255.255.255.0
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

Objectives

Part 1: Configure and Verify DTP

Part 2: Configure and Verify VTP

Background / Scenario

As the number of switches in a network increases, the administration necessary to manage the VLANs and trunks can be challenging. To ease some of the VLAN and trunking configurations, VLAN trunking protocol (VTP) allows a network administration to automate the management of VLANs. Trunk negotiation between network devices is managed by the Dynamic Trunking Protocol (DTP), and is automatically enabled on Catalyst 2960 and Catalyst 3560 switches.

In this activity, you will configure trunk links between the switches. You will configure a VTP server and VTP clients in the same VTP domain. You will also observe the VTP behavior when a switch is in VTP transparent mode. You will assign ports to VLANs and verify end-to-end connectivity with the same VLAN.

Part 1: Configure and Verify DTP

In Part 1, you will configure trunk links among the switches, and you will configure VLAN 999 as the native VLAN.

Step 1: Verify VLAN configuration.

Verify the configured VLANs on the switches.

a. On S1, click the **CLI** tab. At the prompt, enter **enable** and enter the **show vlan brief** command to verify the configured VLANs on S1.

```
S1# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, 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
                                                Gig0/1, Gig0/2
99   Management                       active
999  VLAN0999                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

b. Repeat step a. on S2 and S3. What VLANs are configured on the switches?

Vlans 99 y 999 estan configuradas en todos los switches____________________________________

Step 2: Configure Trunks on S1, S2, and S3.

Dynamic trunking protocol (DTP) manages the trunk links between Cisco switches. Currently all the switchports are in the default trunking mode, which is dynamic auto. In this step, you will change the trunking mode to dynamic desirable for the link between switches S1 and S2. For the link between switches S1 and S3, the link will be set as a static trunk. Use VLAN 999 as the native VLAN in this topology.

a. On switch S1 and switch S2, configure the trunk link to dynamic desirable on the GigabitEthernet 0/1 interface. The configuration of S1 is shown below.

```
S1(config)# interface g0/1
S1(config-if)# switchport mode dynamic desirable
```

b. For the trunk link between S1 and S3, configure a static trunk link on the GigabitEthernet 0/2 interface.

```
S1(config)# interface g0/2
S1(config-if)# switchport mode trunk
S3(config)# interface g0/2
```



```
S3(config-if)# switchport mode trunk
```

c. Verify trunking is enabled on all the switches using the **show interfaces trunk** command.

```
S1# show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      desirable    n-802.1q       trunking      1
Gig0/2      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Gig0/1      1-1005
Gig0/2      1-1005

Port        Vlans allowed and active in management domain
Gig0/1      1,99,999
Gig0/2      1,99,999

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      none
Gig0/2      none
```

What is the native VLAN for these trunks currently? Vlan 1 ____________________

d. Configure VLAN 999 as the native VLAN for the trunk links on S1.

```
S1(config)# interface range g0/1 - 2
S1(config-if-range)# switchport trunk native vlan 999
```

What messages did you receive on S1? How would you correct it?

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/1 (999), with Switch GigabitEthernet0/1 (1).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/2 (999), with Switch GigabitEthernet0/1 (1)

e. On S2 and S3, configure VLAN 999 as the native VLAN.

f. Verify trunking is successfully configured on all the switches. You should be able ping one switch from another switch in the topology using the IP addresses configured on the SVI.

Part 2: Configure and Verify VTP

S1 will be configured as the VTP server and S2 will be configured as a VTP client. All the switches will be configured to be in the VTP domain **CCNA** and use the VTP password **cisco**.

VLANs can be created on the VTP server and distributed to other switches in the VTP domain. In this part, you will create 3 new VLANs on the VTP server, S1. These VLANs will be distributed to S2 using VTP. Observe how the transparent VTP mode behaves.

Step 1: Configure S1 as VTP server.

Configure S1 as the VTP server in the **CCNA** domain with the password **cisco**.

a. Configure S1 as a VTP server.

```
S1(config)# vtp mode server
Setting device to VTP SERVER mode.
```

b. Configure **CCNA** as the VTP domain name.

```
S1(config)# vtp domain CCNA
Changing VTP domain name from NULL to CCNA
```

c. Configure **cisco** as the VTP password.

```
S1(config)# vtp password cisco
Setting device VLAN database password to cisco
```

Step 2: Verify VTP on S1.

a. Use the **show vtp status** command on the switches to confirm that the VTP mode and domain are configured correctly.

```
S1# show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 7
VTP Operating Mode              : Server
VTP Domain Name                 : CCNA
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x8C 0x29 0x40 0xDD 0x7F 0x7A 0x63 0x17
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 192.168.99.1 on interface Vl99 (lowest numbered VLAN interface
found)
```

b. To verify the VTP password, use the **show vtp password** command.

```
S1# show vtp password
VTP Password: cisco
```

Step 3: Add S2 and S3 to the VTP domain.

Before S2 and S3 will accept VTP advertisements from S1, they must belong to the same VTP domain. Configure S2 as a VTP client with **CCNA** as the VTP domain name and **cisco** as the VTP password. Remember that VTP domain names are case sensitive.

a. Configure S2 as a VTP client in the **CCNA** VTP domain with the VTP password **cisco**.

```
S2(config)# vtp mode client
Setting device to VTP CLIENT mode.
S2(config)# vtp domain CCNA
Changing VTP domain name from NULL to CCNA
S2(config)# vtp password cisco
Setting device VLAN database password to cisco
```

b. To verify the VTP password, use the **show vtp password** command.

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

c. Configure S3 to be in the **CCNA** VTP domain with the VTP password **cisco**. Switch S3 will be set in VTP transparent mode.


```
S3(config)# vtp mode Transparent
S3(config)# vtp domain CCNA
Changing VTP domain name from NULL to CCNA
S3(config)# vtp password cisco
Setting device VLAN database password to cisco
```

d. Enter **show vtp status** command on all the switches to answer the following question.

Notice that the configuration revision number is 0 on all three switches. Explain.

El numero de revicion de configuración incrementa en 1 cada vez que una VLAN es agregada, eliminada o modificada. En estos momentos no se ha hecho ninguna configuración adicional, por lo que se encuentra en 0

Step 4: Create more VLANs on S1.

a. On S1, create VLAN 10 and name it Red.

```
S1(config)# vlan 10
S1(config-vlan)# name Red
```

b. Create VLANs 20 and 30 according to the table below.

VLAN Number	VLAN Name
10	Red
20	Blue
30	Yellow

c. Verify the addition of the new VLANs. Enter **show vlan brief** at the privileged EXEC mode.

Which VLANs are configured on S1?

Vlan 1, 10, 20, 39, 99 y 999

d. Confirm configuration changes using the **show vtp status** command on S1 and S2 to confirm that the VTP mode and domain are configured correctly. Output for S2 is shown here:

```
S2# show vtp status
VTP Version                     : 2
Configuration Revision          : 6
Maximum VLANs supported locally : 255
Number of existing VLANs        : 10
VTP Operating Mode              : Client
VTP Domain Name                 : CCNA
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xE6 0x56 0x05 0xE0 0x7A 0x63 0xFB 0x33
Configuration last modified by 192.168.99.1 at 3-1-93 00:21:07
```

How many VLANs are configured on S2? Does S2 have the same VLANs as S1? Explain.

S2 tiene 10 vlans, las mismas que s1. Porque s1 es el vtp server y s2 es un vtp client en el dominio de CCNA, s2 recibe la información de vlans del s1.

Step 5: Observe VTP transparent mode.

S3 is currently configured as VTP transparent mode.

a. Use **show vtp status** command to answer the following question.

How many VLANs are configured on S3 currently? What is the configuration revision number? Explain your answer.

Actualmente hay 7 vlans en s3, el número de revisión de configuración es 0 porque s3 es un modo transparente y la configuración de vlans no ha sido cambiada desde el inicio del interruptor

How would you change the number of VLANs on S3?

Mientras que s3 es modo transparente, no podra implementar la información de vlans del vtp server, por lo que todos los cambios en las vlans deberán ser configurados manualmente o s3 podría ser cambiado a vtp cliente para implementar la información de vlans del vtp server

b. Change VTP mode to client on S3.

Use show commands to verify the changes on VTP mode. How many VLANs exists on S3 now?

10

Note: VTP advertisements are flooded throughout the management domain every five minutes, or whenever a change occurs in VLAN configurations. To accelerate this process, you can switch between Realtime mode and Simulation mode until the next round of updates. However, you may have to do this multiple times because this will only forward Packet Tracer's clock by 10 seconds each time. Alternatively, you can change one of the client switches to transparent mode and then back to client mode.

Step 6: Assign VLANs to Ports

Use the **switchport mode access** command to set access mode for the access links. Use the **switchport access vlan** *vlan-id* command to assign a VLAN to an access port.

Ports	Assignments	Network
S2 F0/1 – 8 S3 F0/1 – 8	VLAN 10 (Red)	192.168.10.0 /24
S2 F0/9 – 16 S3 F0/9 – 16	VLAN 20 (Blue)	192.168.20.0 /24
S2 F0/17 – 24 S3 F0/17 – 24	VLAN 30 (Yellow)	192.168.30.0 /24

a. Assign VLANs to ports on S2 using assignments from the table above.

```
S2(config-if)# interface range f0/1 - 8
S2(config-if-range)# switchport mode access
S2(config-if-range)# switchport access vlan 10
S2(config-if-range)# interface range f0/9 -16
S2(config-if-range)# switchport mode access
S2(config-if-range)# switchport access vlan 20
S2(config-if-range)# interface range f0/17 - 24
S2(config-if-range)# switchport mode access
S2(config-if-range)# switchport access vlan 30
```

b. Assign VLANs to ports on S3 using assignment from the table above.

Step 7: Verify end to end connectivity.

a. From PC0 ping PC5.

b. From PC1 ping PC4.

c. From PC2 ping PC3.