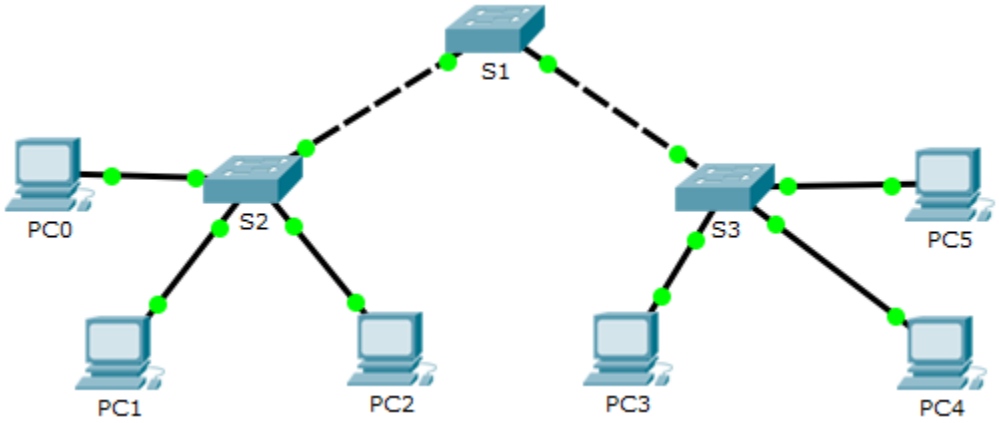
Packet Tracer – Troubleshoot VTP and DTP

Topology



Addressing Table

Device	IP Address	Subnet Mask
PC0	172.16.10.1	255.255.255.0
PC1	172.16.20.1	255.255.255.0
PC2	172.16.30.1	255.255.255.0
PC3	172.16.30.2	255.255.255.0
PC4	172.16.20.2	255.255.255.0
PC5	172.16.10.2	255.255.255.0
S1	172.16.99.1	255.255.255.0
S2	172.16.99.2	255.255.255.0
S3	172.16.99.3	255.255.255.0

Objectives

Part 1: Troubleshoot DTP

Part 2: Troubleshoot VTP

Background / Scenario

In this activity, the switches S2 and S3 are not implementing VTP information. You will verify that DTP and VTP configurations are correctly implemented. When all the issues are resolved, the PCs in the same VLAN will be able to communicate with each other.

Part 1: Troubleshoot DTP

In Part 1, you will troubleshoot the trunk links among the switches. You will verify that permanent trunk links are used between the switches.

a. Enter **show interfaces trunk** at the privileged EXEC prompt on all the switches to determine the status of the trunk links. How many trunk links are configured currently?

no trunk

b. Enter **show interfaces g0/1 switchport** at the privileged EXEC prompt on S1. Do the same for g0/2 interface on S1.

What is the operational mode on the GigabitEthernet interfaces on S1?

c. Repeat the commands for g0/1 on S2 and g0/2 on S3.

Correct the trunk links. Record the commands you used to correct the trunking issue.

s1:
switchport mode trunk on g0/1, g0/2
s2:
switchport mode trunk on g0/1
s3:
switchport mode trunk on g0/2

d. Verify the trunk links using the **show** commands.

Part 2: Troubleshoot VTP

S1 will be configured as the VTP server. S2 and S3 will be configured as VTP clients, and will be receiving VTP updates from S1. The VTP domain should be **CCNA** and the VTP password should be **cisco**. Currently all the desired VLANs are already configured on S1.

Step 1: Verify VLAN information

Use the **show vlan brief** command on all the switches. Do all the switches have the same number of VLANs? How many does each switch have?

no, 10 on s1, and 7 on others

Step 2: Verify VTP configurations.

Use the **show vtp status** and **show vtp password** commands on all the switches to verify the VTP status.

Record the VTP status information in the table below.

Device	Domain Name	Operating Mode	VTP Password
S1	no domain	transparent	no pswd
S2	ccna	transparent	no pswd
S3	CCNA	transparent	Cisco

Step 3: Correct the VTP configurations.

Record the commands used to correct the VTP configurations.

S1(config)#vtp mode server
Setting device to VTP SERVER mode.
S1(config)#vtp domain CCNA
Changing VTP domain name from NULL to CCNA
S1(config)#vtp pa
S1(config)#vtp password cisco
Setting device VLAN database password to cisco

Step 4: Verify port assignment.

The switchports connecting to the PCs need to be configured in the correct VLANs so the PCs can communicate with each other.

Use the **show vlan brief** command on S2 and S3 to determine if VLANs have been assigned to the switchports. Which VLAN is associated with these switchports?

Ports	Assignments	Network
S2 F0/1 S3 F0/8	VLAN 10 (Staff)	172.16.10.0/24
S2 F0/9 S3 F0/16	VLAN 20 (Student)	172.16.20.0 /24
S2 F0/17 S3 F0/24	VLAN 30 (Faculty)	172.16.30.0 /24

Using the table above, correct the VLAN assignments on S2 and S3. Record the VLAN assignment configurations below.

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

Step 5: Verify end to end connectivity.

a. From PC0 ping PC5.

b. From PC1 ping PC4.

c. From PC2 ping PC3.