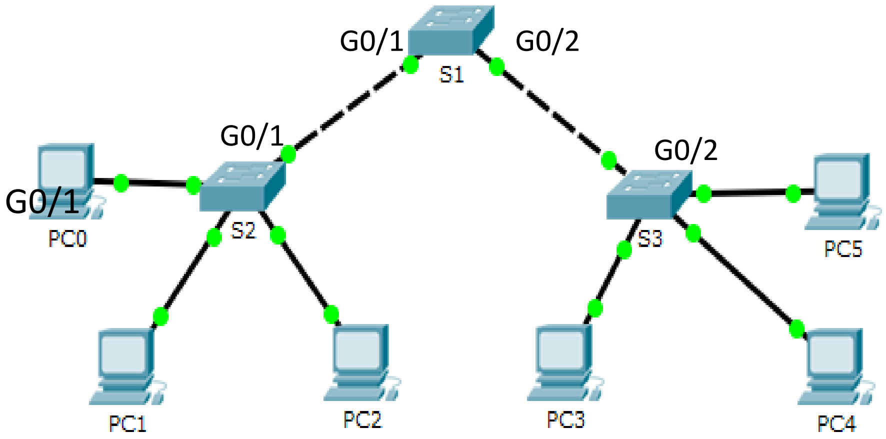
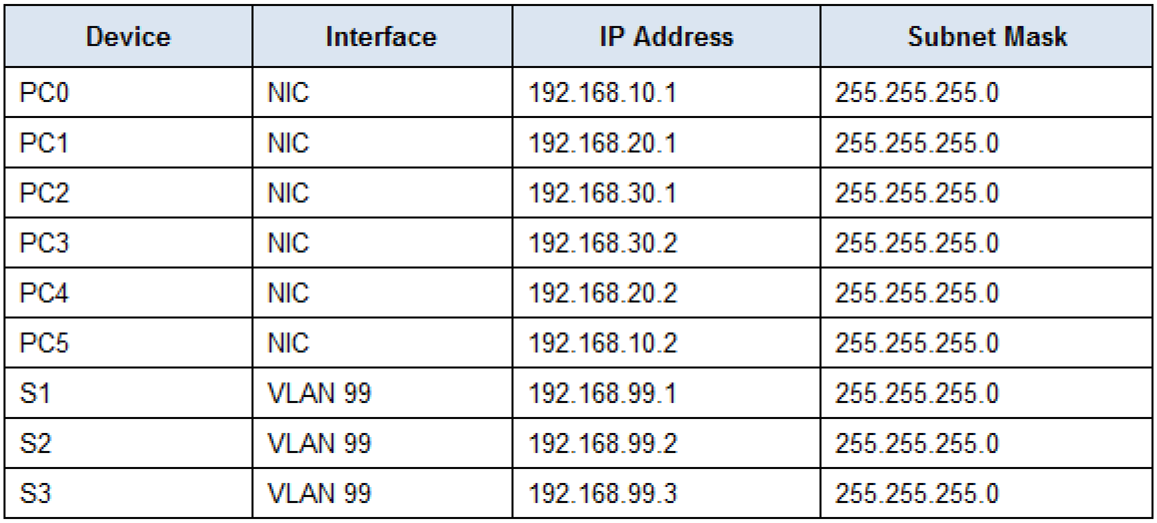
Configure VLANs, VTP, and DTP



Packet Tracer – Configure VLANs, VTP and DTP
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.

Steo 0: Create Vlan 999 (table)

Step 1: Verify VLAN configuration.

Verify the configured VLANs on the 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.

Part 2: Configure and Verify VTP

S1 will be configured as the VTP server and S2 will be configured as VTP clients. 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.

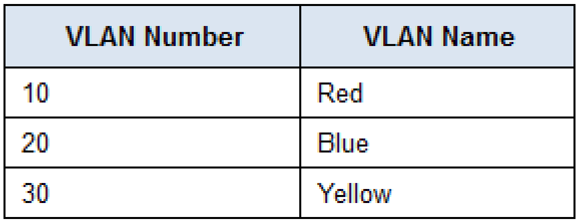
Configure S1 as the VTP server in the CCNA domain with the password cisco.

Step 2: Verify VTP on S1.

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 and S3 as VTP clients with CCNA as the VTP domain name and cisco as the VTP password. Remember that VTP domain names are case sensitive.

Step 4: Create more VLANs on S1 (see table).



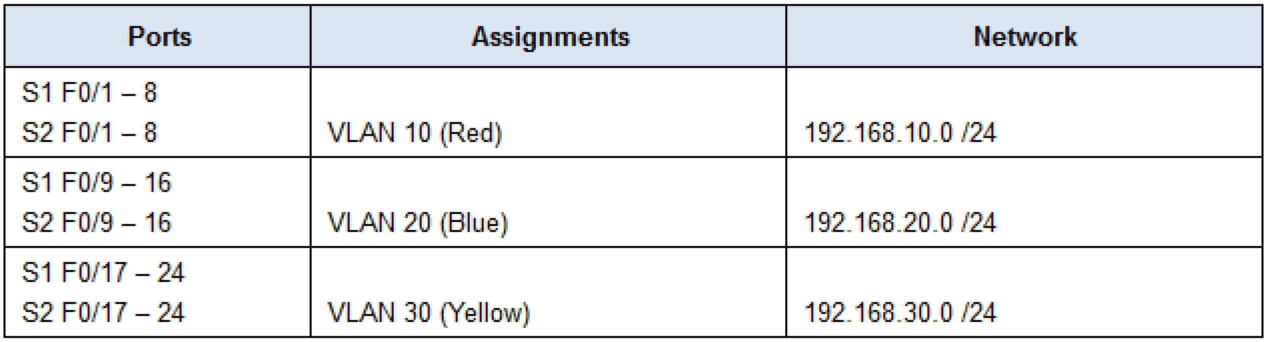
VLAN Number	VLAN Name
10	Red
20	Blue
30	Yellow

Step 5: Observe VTP transparent mode on S3.

S3 is currently configured as VTP transparent 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
S1 F0/1 – 8 S2 F0/1 – 8	VLAN 10 (Red)	192.168.10.0 /24
S1 F0/9 – 16 S2 F0/9 – 16	VLAN 20 (Blue)	192.168.20.0 /24
S1 F0/17 – 24 S2 F0/17 – 24	VLAN 30 (Yellow)	192.168.30.0 /24

Step 7: Verify end to end connectivity.

a. From PC0 ping PC5.

b. From PC1 ping PC4.

c. From PC2 ping PC3.