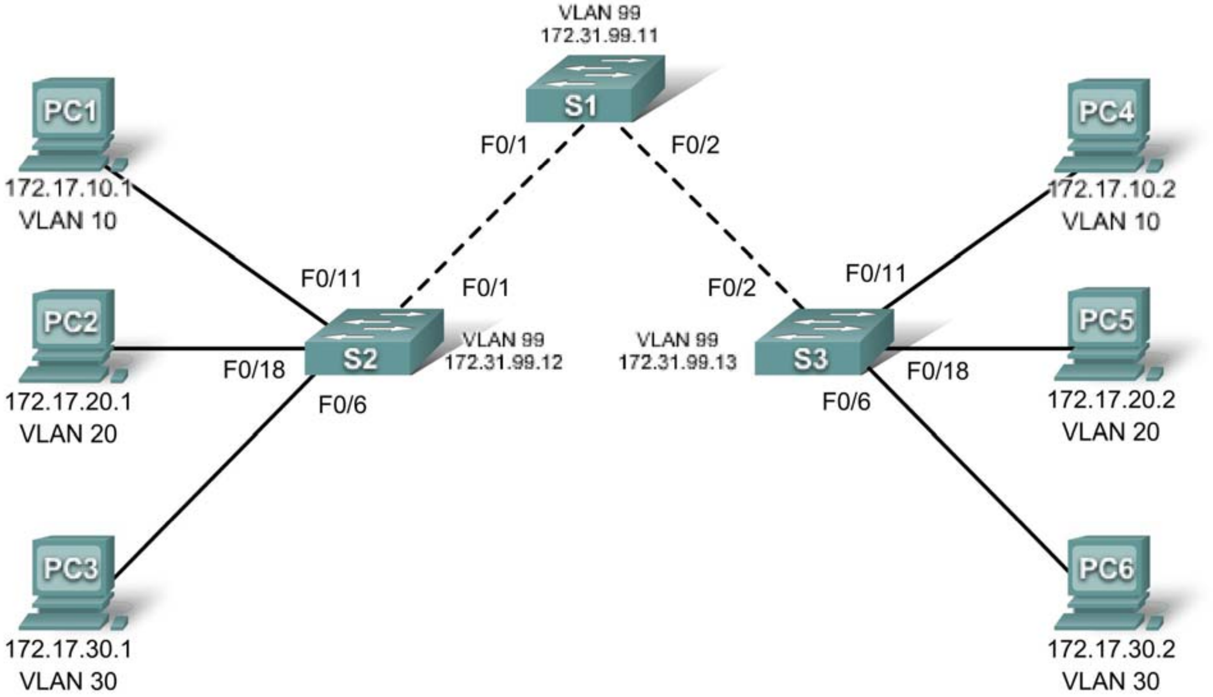
Lab 4.4.2: VTP Configuration Challenge

Topology



Addressing Table

Device (Hostname)	Interface	IP Address	Subnet Mask	Default Gateway
S1	**VLAN 99**	172.31.99.11	255.255.255.0	N/A
S2	**VLAN 99**	172.31.99.12	255.255.255.0	N/A
S3	**VLAN 99**	172.31.99.13	255.255.255.0	N/A
PC1	**NIC**	172.31.10.1	255.255.255.0	
PC2	**NIC**	172.31.20.1	255.255.255.0	
PC3	**NIC**	172.31.30.1	255.255.255.0	
PC4	**NIC**	172.31.10.2	255.255.255.0	
PC5	**NIC**	172.31.20.2	255.255.255.0	
PC6	**NIC**	172.31.30.2	255.255.255.0	

Port Assignments (Switches 2 and 3)

Ports	Assignment	Network
Fa0/1 – 0/5	802.1q Trunks	
Fa0/11 – 0/17	VLAN 10 – Engineering	172.31.10.0 /24
Fa0/18 – 0/24	VLAN 20 – Sales	172.31.20.0 /24
Fa0/6 – 0/10	VLAN 30 – Administration	172.31.30.0 /24
None	VLAN 99 – Network Mgmt	172.31.99.0 /24

Learning Objectives

Upon completion of this lab, you will be able to:

- Cable a network according to the topology diagram.
- Erase the startup configuration and reload a switch to the default state.
- Perform basic configuration tasks on a switch.
- Configure VLAN Trunking Protocol (VTP) on all switches.
- Enable trunking on inter-switch connections.
- Verify trunk configuration.
- Modify VTP modes and observe the impact.
- Create VLANs on the VTP server, and distribute this VLAN information to switches in the network.
- Explain the differences in operation between VTP transparent mode, server mode, and client mode.
- Assign switch ports to the VLANs.
- Save the VLAN configuration.

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.

Step 2: Clear any existing configurations on the switches.

Step 3: Disable all ports by using the shutdown command.

Step 4: Re-enable the user ports on S2 and S3 and put those ports in access mode. Refer to the topology diagram to determine which ports are connected to end-user devices.

Task 2: Perform Basic Switch Configurations.

Configure the S1, S2, and S3 switches according to the following guidelines and save all your configurations:

- Configure the switch hostname as indicated on the topology.
- Disable DNS lookup.
- Configure an EXEC mode password of **class**.
- Configure a password of **cisco** for console connections.

- Configure a password of **cisco** for vty connections.

Task 3: Configure the Ethernet Interfaces on the Host PCs

Configure the Ethernet interfaces of PC1 through PC6 with the IP addresses indicated in the addressing table at the beginning of the lab.

Task 4: Configure VTP on the Switches

Step 1: Check the current VTP settings on the three switches.

Step 2: Configure the operating mode, the domain name, and VTP password on all three switches.

Step 3: Configure trunking and the native VLAN for the trunking ports on all three switches.

Configure ports Fa0/1 through Fa0/5 in trunking mode. Configure VLAN 99 as the native VLAN for these trunks.

Step 4: Configure port security on the S2 and S3 access ports.

Configure ports Fa0/6, Fa0/11, and Fa0/18 on S2 and S3 so that they allow a maximum of two hosts to connect to these ports and learn the MAC addresses of the hosts dynamically.

Step 5: Configure VLANs on the VTP server.

When you are done, verify that all four VLANs have been created on S1.

Step 6: Check if the VLANs created on S1 have been distributed to S2 and S3.

Step 7: Configure the management interface address on all three switches.

Configure all three switches with the IP addresses identified in the addressing table at the beginning of the lab. Assign these addresses to the network management VLAN (VLAN 99).

Step 8: Assign switch ports to VLANs.

Refer to the port assignment table at the beginning of the lab to assign ports to VLANs.

Step 9: Verify that the trunks are operating correctly.

Task 5: Configure VTP Pruning on the Switches

Confirm the VTP pruning configuration on each switch.

Task 6: Clean Up

Erase the configurations and reload the switches. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.