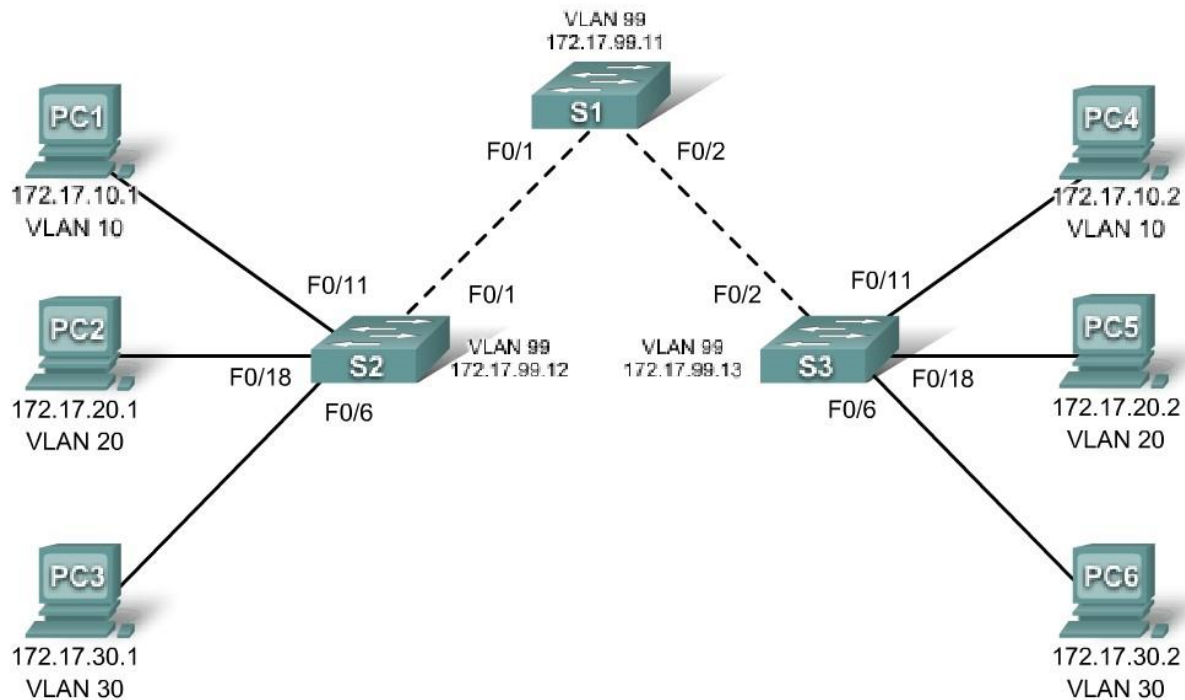**Felix Rohrer**

Lab 4.4.2 Challenge VTP Configuration

Topology

Addressing Table

Device (Hostname)	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 99	172.17.99.11	255.255.255.0	N/A
S2	VLAN 99	172.17.99.12	255.255.255.0	N/A
S3	VLAN 99	172.17.99.13	255.255.255.0	N/A
PC1	NIC	172.17.10.1	255.255.255.0	
PC2	NIC	172.17.20.1	255.255.255.0	
PC3	NIC	172.17.30.1	255.255.255.0	
PC4	NIC	172.17.10.2	255.255.255.0	
PC5	NIC	172.17.20.2	255.255.255.0	
PC6	NIC	172.17.30.2	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	172.17.10.0 /24
Fa0/18 – 0/24	VLAN 20 – sales	172.17.20.0 /24
Fa0/6 – 0/10	VLAN 30 – administration	172.17.30.0 /24
None	VLAN 99 – network management	172.17.99.0 /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.

You can use any current switch in your lab as long as it has the required interfaces shown in the topology diagram. The output shown in this lab is based on 2960 switches. Other switch types may produce different output. If you are using older switches, then some commands may be different or unavailable.

Set up console connections to all three switches.

Step 2: Clear any existing configurations on the switches.

Erase existing configurations, VLANs, and reload the switch. Use the **show vlan** command to confirm that only default VLANs exist and that all ports are assigned to VLAN 1.

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

Task 2: Perform Basic Switch Configurations.

Step 1: Complete basic configuration of switches S1, S2, and S3.

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.

- Save running-configuration to startup-configuration.

Step 2: 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 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

VTP allows the network administrator to control the instances of VLANs on the network by creating VTP domains. Within each VTP domain, one or more switches are configured as VTP servers. VLANs are then created on the VTP server and pushed to the other switches in the domain. Common VTP configuration tasks are operating mode, domain, and password. In this lab, you will be configuring S1 as a VTP server, with S2 and S3 configured as VTP clients.

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

What is the current (default) VTP operating mode on the switches? server

What is the configuration revision on S1 and S2? 0

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

Set the VTP domain name to **access** and the VTP password to **lab4** on all three switches**.** Configure S1 in server mode, and S2 and S3 in client mode.

Note: The VTP domain name can be learned by a client switch from a server switch, but only if the client switch domain is in the null state. It does not learn a new name if one has been previously set. For that reason, it is good practice to manually configure the domain name on all switches to ensure that the domain name is configured correctly. Switches in different VTP domains do not exchange VLAN information. Recall that VTP domain names and passwords are case-sensitive.

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. You can use the **interface range** command to simplify this task. Do not forget to enable the trunk interfaces.

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.

There are four VLANS required in this lab:

1. VLAN 99 (network management)

2. VLAN 10(engineering)

3. VLAN 20 (sales)

4. VLAN 30 (administration)

Configure these VLANs only 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.

Use the **show vlan brief** command on S2 and S3 to determine if the VTP server has pushed its VLAN configuration to all these switches.

Are the same VLANs configured on all switches? **nein**

Explain why S2 and S3 have the same VLAN configurations at this point

S3 ist im transparent Mode und übernimmt somit die Config nicht.

Sobald S3 ebenfalls im Client Mode ist, übernimmt er die VLan Config

Step 7: Configure the management interface address on all three switches according to the addressing table at the beginning of the lab.

Assign these addresses to the network management VLAN (VLAN 99).

Verify that the switches are correctly configured by pinging between them. From S1, ping the management interface on S2 and S3. From S2, ping the management interface on S3.

Were the pings successful? **yes** If not, troubleshoot the switch configurations and resolve.

Step 8: Assign switch ports to VLANs.

Refer to the port assignment table at the beginning of the lab to assign ports to VLANs. Use the **interface range** command to simplify this task. Note that port assignments are not configured through VTP. Port assignments must be configured on each switch manually or dynamically using a VMPS server. Save the configuration when you are done.

Step 9: Verify that the trunks are operating correctly.

From PC1, attempt to ping PC4, PC5, and PC6.

Were any of the pings successful? **PC4 ok, PC5/6 fail**

Why did some of the pings fail? **Anderes VLan resp. Subnet**

Which hosts could be reached from PC3? **PC6**