# Lab 4.4.1: Basic VTP Configuration

## Topology Diagram

## E3_4_4_1_1_032607

## 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** | 172.17.10.21 | 255.255.255.0 | 172.17.10.1 |
| **PC2** | **NIC** | 172.17.20.22 | 255.255.255.0 | 172.17.20.1 |
| **PC3** | **NIC** | 172.17.30.23 | 255.255.255.0 | 172.17.30.1 |
| **PC4** | **NIC** | 172.17.10.24 | 255.255.255.0 | 172.17.10.1 |
| **PC5** | **NIC** | 172.17.20.25 | 255.255.255.0 | 172.17.20.1 |
| **PC6** | **NIC** | 172.17.30.26 | 255.255.255.0 | 172.17.30.1 |

## Port Assignments (Switches 2 and 3)

|  |  |  |
| --- | --- | --- |
| **Ports** | **Assignment** | **Network** |
| Fa0/1 – 0/5 | 802.1q Trunks (Native VLAN 99) | 172.17.99.0 /24 |
| Fa0/6 – 0/10 | VLAN 30 – Guest (Default) | 172.17.30.0 /24 |
| Fa0/11 – 0/17 | VLAN 10 – Faculty/Staff | 172.17.10.0 /24 |
| Fa0/18 – 0/24 | VLAN 20 – Students | 172.17.20.0 /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
* Enable VTP pruning on the network
* Explain how pruning reduces unnecessary broadcast traffic on the LAN

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. 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.

You will notice in the Addressing Table that the PCs have been configured with a default gateway IP address. This would be the IP address of the local router which is not included in this lab scenario. The default gateway, the router would be needed for PCs in different VLANS to be able to communicate. This is discussed in a later chapter.

Set up console connections to all three switches.

Step 2: Clear any existing configurations on the switches.

If necessary, refer to Lab 2.5.1, Appendix 1, for the procedure to clear switch configurations and VLANs. Use the **show vlan** command to confirm that only default VLANs exist and that all ports are assigned to VLAN 1.

Switch#**show vlan**

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

Gig1/1, Gig1/2

1002 fddi-default active

1003 token-ring-default active

1004 fddinet-default active

1005 trnet-default active

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

Repeat these commands for each switch in the topology.

Switch(config)#**interface range fa0/1-24**

Switch(config-if-range)#**shutdown**

Switch(config-if-range)#**interface range gi0/1-2**

Switch(config-if-range)#**shutdown**

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.

(Output for S1 shown)

Switch>**enable**

Switch#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#**hostname S1**

S1(config)#**enable secret class**

S1(config)#**no ip domain-lookup**

S1(config)#**line console 0**

S1(config-line)#**password cisco**

S1(config-line)#**login**

S1(config-line)#**line vty 0 15**

S1(config-line)#**password cisco**

S1(config-line)#**login**

S1(config-line)#**end**

%SYS-5-CONFIG\_I: Configured from console by console

S1#**copy running-config startup-config**

Destination filename [startup-config]?

Building configuration...

[OK]

Step 2: Re-enable the user ports on S2 and S3.

Configure the user ports in access mode. Refer to the topology diagram to determine which ports are connected to end-user devices.

S2(config)#**interface fa0/6**

S2(config-if)#**switchport mode access**

S2(config-if)#**no shutdown**

S2(config-if)#**interface fa0/11**

S2(config-if)#**switchport mode access**

S2(config-if)#**no shutdown**

S2(config-if)#**interface fa0/18**

S2(config-if)#**switchport mode access**

S2(config-if)#**no shutdown**

S3(config)#**interface fa0/6**

S3(config-if)#**switchport mode access**

S3(config-if)#**no shutdown**

S3(config-if)#**interface fa0/11**

S3(config-if)#**switchport mode access**

S3(config-if)#**no shutdown**

S3(config-if)#**interface fa0/18**

S3(config-if)#**switchport mode access**

S3(config-if)#**no shutdown**

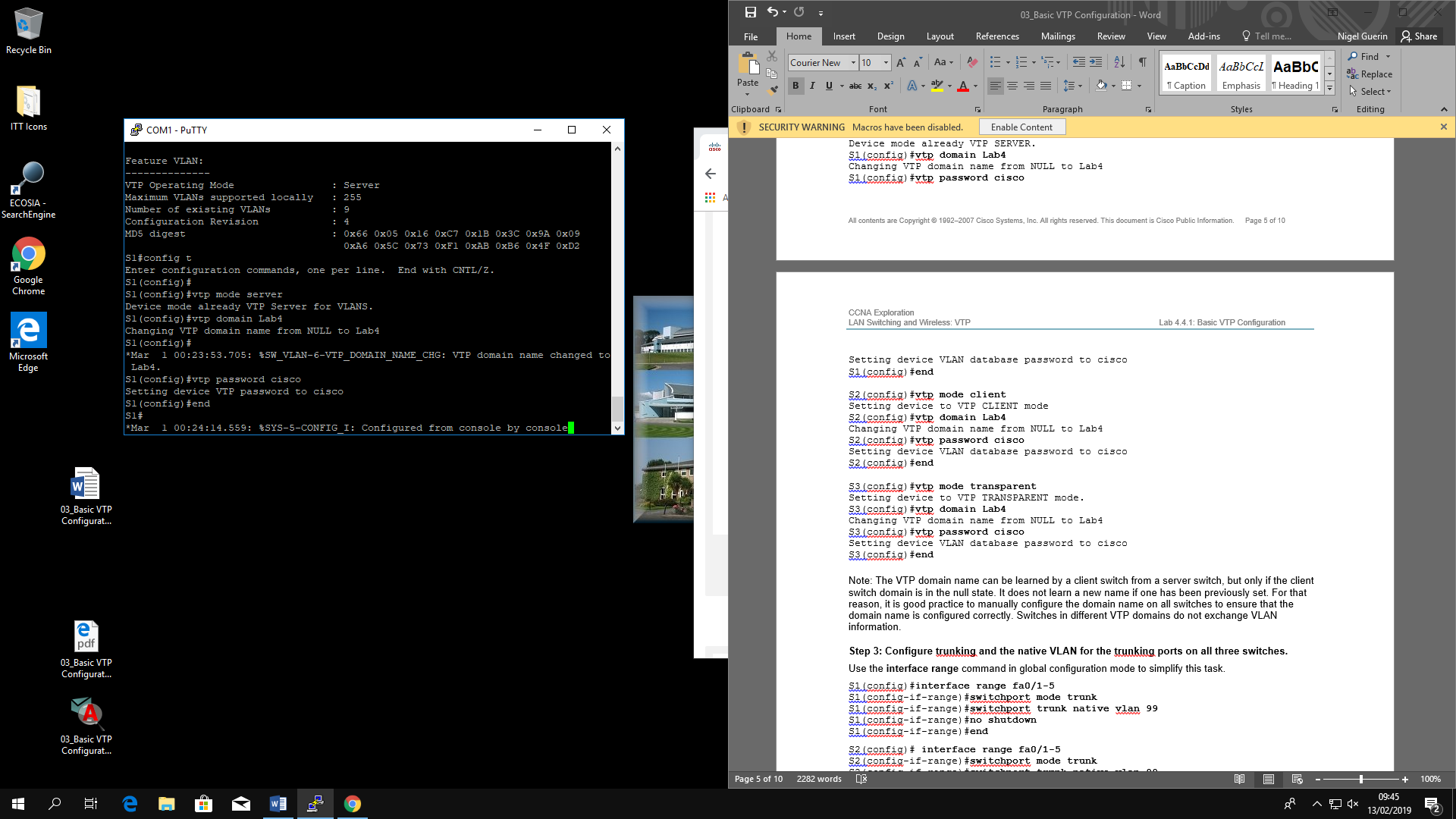
Step 3: Re-enable the trunk ports on S1, S2 and S3

S1(config)#**interface fa0/1** S1(config-if)#**no shutdown**  S1(config)#**interface fa0/2**  S1(config-if)#**no shutdown**

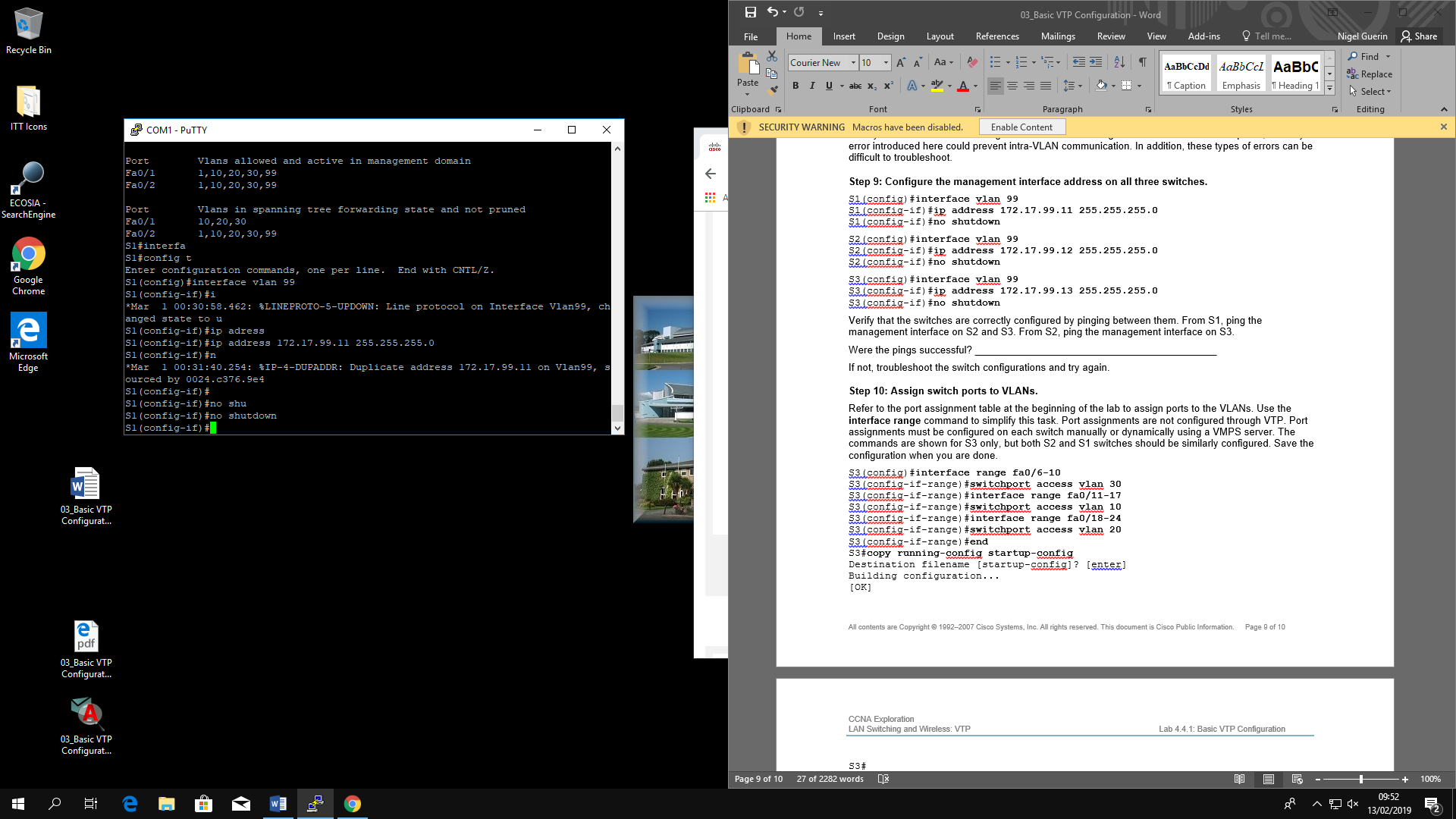
S2(config)#**interface fa0/1**  S2(config-if)#**no shutdown**

S3(config)#**interface fa0/2**  S3(config-if)#**no shutdown**

**Setting password:**



**No shutdown:**



Task 3: Configure the Ethernet Interfaces on the Host PCs

Configure the Ethernet interfaces of PC1, PC2, PC3, PC4, PC5, and PC6 with the IP addresses and default gateways indicated in the addressing table at the beginning of the lab.

Verify that PC1 can ping PC4, PC2 can ping PC5, and that PC3 can ping PC6.

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 setting the operating mode, domain, and password. In this lab, you will be using S1 as the VTP server, with S2 and S3 configured as VTP clients or in VTP transparent mode.

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

S1#**show vtp status**

VTP Version : 2

Configuration Revision : 0

Maximum VLANs supported locally : 255

Number of existing VLANs : 5

VTP Operating Mode : Server

VTP Domain Name :

VTP Pruning Mode : Disabled

VTP V2 Mode : Disabled

VTP Traps Generation : Disabled

MD5 digest : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD

Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00

Local updater ID is 0.0.0.0 (no valid interface found)

S2#**show vtp status**

VTP Version : 2

Configuration Revision : 0

Maximum VLANs supported locally : 255

Number of existing VLANs : 5

VTP Operating Mode : Server

VTP Domain Name :

VTP Pruning Mode : Disabled

VTP V2 Mode : Disabled

VTP Traps Generation : Disabled

MD5 digest : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD

Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00

Local updater ID is 0.0.0.0 (no valid interface found)

S3#**show vtp status**

VTP Version : 2

Configuration Revision : 0

Maximum VLANs supported locally : 255

Number of existing VLANs : 5

VTP Operating Mode : Server

VTP Domain Name :

VTP Pruning Mode : Disabled

VTP V2 Mode : Disabled

VTP Traps Generation : Disabled

MD5 digest : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD

Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00

Note that all three switches are in server mode. Server mode is the default VTP mode for most Catalyst switches.

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

Set the VTP domain name to **Lab4** and the VTP password to **cisco** on all three switches**.** Configure S1 in server mode, S2 in client mode, and S3 in transparent mode.

S1(config)#**vtp mode server**

Device mode already VTP SERVER.

S1(config)#**vtp domain Lab4**

Changing VTP domain name from NULL to Lab4

S1(config)#**vtp password cisco**

Setting device VLAN database password to cisco

S1(config)#**end**

S2(config)#**vtp mode client**

Setting device to VTP CLIENT mode

S2(config)#**vtp domain Lab4**

Changing VTP domain name from NULL to Lab4

S2(config)#**vtp password cisco**

Setting device VLAN database password to cisco

S2(config)#**end**

S3(config)#**vtp mode transparent**

Setting device to VTP TRANSPARENT mode.

S3(config)#**vtp domain Lab4**

Changing VTP domain name from NULL to Lab4

S3(config)#**vtp password cisco**

Setting device VLAN database password to cisco

S3(config)#**end**

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.

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

Use the **interface range** command in global configuration mode to simplify this task.

S1(config)#**interface range fa0/1-5**

S1(config-if-range)#**switchport mode trunk**

S1(config-if-range)#**switchport trunk native vlan 99**

S1(config-if-range)#**no shutdown**

S1(config-if-range)#**end**

S2(config)# **interface range fa0/1-5**

S2(config-if-range)#**switchport mode trunk**

S2(config-if-range)#**switchport trunk native vlan 99**

S2(config-if-range)#**no shutdown**

S2(config-if-range)#**end**

S3(config)# **interface range fa0/1-5**

S3(config-if-range)#**switchport mode trunk**

S3(config-if-range)#**switchport trunk native vlan 99**

S3(config-if-range)#**no shutdown**

S3(config-if-range)#**end**

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

Configure ports fa0/6, fa0/11, and fa0/18 so that they allow only a single host and learn the MAC address of the host dynamically.

S2(config)#**interface fa0/6**

S2(config-if)#**switchport port-security**

S2(config-if)#**switchport port-security maximum 1**

S2(config-if)#**switchport port-security mac-address sticky**

S2(config-if)#**interface fa0/11**

S2(config-if)#**switchport port-security**

S2(config-if)#**switchport port-security maximum 1**

S2(config-if)#**switchport port-security mac-address sticky**

S2(config-if)#**interface fa0/18**

S2(config-if)#**switchport port-security**

S2(config-if)#**switchport port-security maximum 1**

S2(config-if)#**switchport port-security mac-address sticky**

S2(config-if)#**end**

S3(config)#**interface fa0/6**

S3(config-if)#**switchport port-security**

S3(config-if)#**switchport port-security maximum 1**

S3(config-if)#**switchport port-security mac-address sticky**

S3(config-if)#**interface fa0/11**

S3(config-if)#**switchport port-security**

S3(config-if)#**switchport port-security maximum 1**

S3(config-if)#**switchport port-security mac-address sticky**

S3(config-if)#**interface fa0/18**

S3(config-if)#**switchport port-security**

S3(config-if)#**switchport port-security maximum 1**

S3(config-if)#**switchport port-security mac-address sticky**

S3(config-if)#**end**

Step 5: Configure VLANs on the VTP server.

There are four additional VLANS required in this lab:

* VLAN 99 (management)
* VLAN 10 (faculty/staff)
* VLAN 20 (students)
* VLAN 30 (guest)

Configure these on the VTP server.

S1(config)#**vlan 99**

S1(config-vlan)#**name management**

S1(config-vlan)#**exit**

S1(config)#**vlan 10**

S1(config-vlan)#**name faculty/staff**

S1(config-vlan)#**exit**

S1(config)#**vlan 20**

S1(config-vlan)#**name students**

S1(config-vlan)#**exit**

S1(config)#**vlan 30**

S1(config-vlan)#**name guest**

S1(config-vlan)#**exit**

Verify that the VLANs have been created on S1 with the **show vlan brief** command.

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 the switches.

S2#**show vlan brief**VLAN Name Status Ports

---- -------------------------------- --------- -----------------------------

1 default active Fa0/1, Fa0/2, 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, Gi0/1

Gi0/2

10 faculty/staff active

20 students active

30 guest active

99 management active

S3#**show vlan brief**

VLAN Name Status Ports

---- -------------------------------- --------- -----------------------------

1 default active Fa0/1, Fa0/2, 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, Gi0/1

Gi0/2

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

Are the same VLANs configured on all switches? Yes

Explain why S2 and S3 have different VLAN configurations at this point. S3 does not participate in the **VTP** Domain.

Step 7: Create a new VLAN on switch 2 and 3.

S2(config)#**vlan 88**

%VTP VLAN configuration not allowed when device is in CLIENT mode.

S3(config)#**vlan 88**

S3(config-vlan)#**name test**

S3(config-vlan)#

Why are you prevented from creating a new VLAN on S2 but not S3? The client does not have permission to change the names of the vlan’s being used

Delete VLAN 88 from S3.

S3(config)#**no vlan 88**

Step 8: Manually configure VLANs.

Configure the four VLANs identified in Step 5 on switch S3.

S3(config)#**vlan 99**

S3(config-vlan)#**name management**

S3(config-vlan)#**exit**

S3(config)#**vlan 10**

S3(config-vlan)#**name faculty/staff**

S3(config-vlan)#**exit**

S3(config)#**vlan 20**

S3(config-vlan)#**name students**

S3(config-vlan)#**exit**

S3(config)#**vlan 30**

S3(config-vlan)#**name guest**

S3(config-vlan)#**exit**

Here you see one of the advantages of VTP. Manual configuration is tedious and error prone, and any error introduced here could prevent intra-VLAN communication. In addition, these types of errors can be difficult to troubleshoot.

Step 9: Configure the management interface address on all three switches.

S1(config)#**interface vlan 99**

S1(config-if)#**ip address 172.17.99.11 255.255.255.0**

S1(config-if)#**no shutdown**

S2(config)#**interface vlan 99**

S2(config-if)#**ip address 172.17.99.12 255.255.255.0**

S2(config-if)#**no shutdown**

S3(config)#**interface vlan 99**

S3(config-if)#**ip address 172.17.99.13 255.255.255.0**

S3(config-if)#**no shutdown**

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 try again.

Step 10: Assign switch ports to VLANs.

Refer to the port assignment table at the beginning of the lab to assign ports to the VLANs. Use the **interface range** command to simplify this task. Port assignments are not configured through VTP. Port assignments must be configured on each switch manually or dynamically using a VMPS server. The commands are shown for S3 only, but both S2 and S1 switches should be similarly configured. Save the configuration when you are done.

S3(config)#**interface range fa0/6-10**

S3(config-if-range)#**switchport access vlan 30**

S3(config-if-range)#**interface range fa0/11-17**

S3(config-if-range)#**switchport access vlan 10**

S3(config-if-range)#**interface range fa0/18-24**

S3(config-if-range)#**switchport access vlan 20**

S3(config-if-range)#**end**

S3#**copy running-config startup-config**

Destination filename [startup-config]? [enter]

Building configuration...

[OK]

S3#

Task 5: Configure VTP Pruning on the Switches

VTP pruning allows a VTP server to suppress IP broadcast traffic for specific VLANs to switches that do not have any ports in that VLAN. By default, all unknown unicasts and broadcasts in a VLAN are flooded over the entire VLAN. All switches in the network receive all broadcasts, even in situations in which few users are connected in that VLAN. VTP pruning is used to eliminate or prune this unnecessary traffic. Pruning saves LAN bandwidth because broadcasts do not have to be sent to switches that do not need them.

Pruning is configured on the server switch with the **vtp pruning** command in global configuration mode. The configuration is pushed to client switches.

Confirm VTP pruning configuration on each switch using the **show vtp status** command. VTP pruning mode should be enabled on each switch.

S1#**show vtp status**

VTP Version : 2

Configuration Revision : 17

Maximum VLANs supported locally : 255

Number of existing VLANs : 9

VTP Operating Mode : Server

VTP Domain Name : Lab4

VTP Pruning Mode : Enabled

<output omitted>

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.