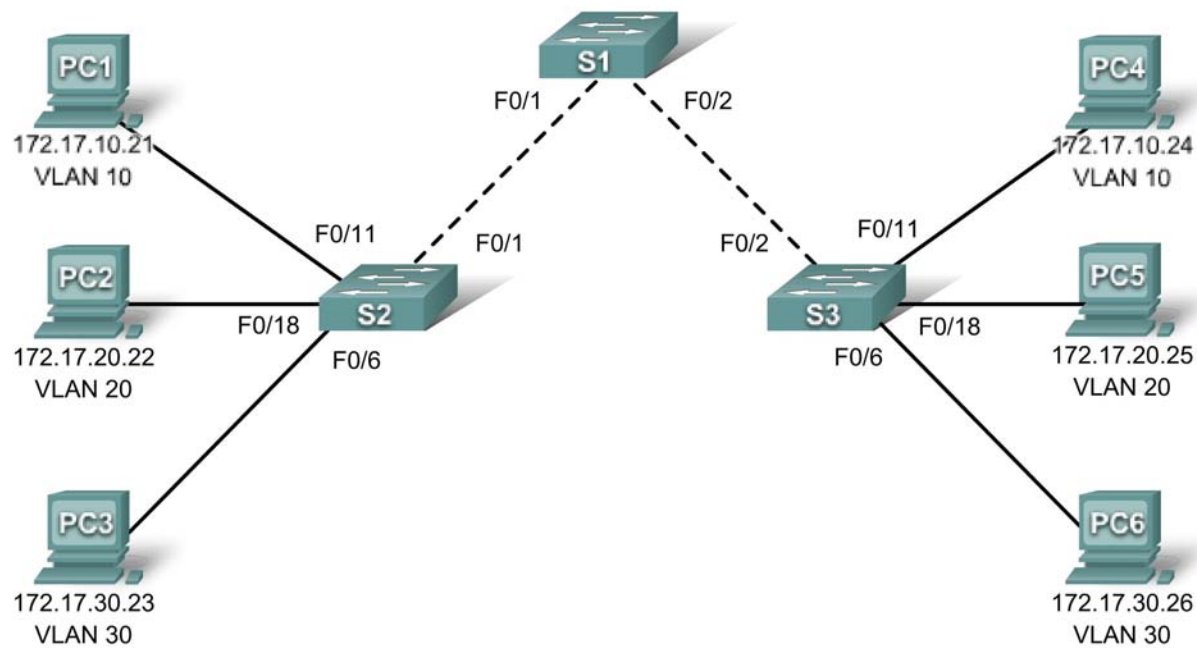


## PT Activity 4.4.1: Basic VTP Configuration

### Topology Diagram



### Addressing Table

Device	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 (S2 and S3)

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

- Perform basic switch configurations.
- Configure the Ethernet interfaces on the host PCs.
- Configure VTP and security on the switches.

## Introduction

In this activity, you will perform basic switch configurations, configure VTP, trunking, learn about VTP modes, create and distribute VLAN information and assign ports to VLANs. The initial network opens in a secure state with all ports administratively shutdown.

## Task 1: 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 encrypted privileged EXEC mode password of **class**.
- Configure a password of **cisco** for console connections.
- Configure a password of **cisco** for vty connections.

```
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]
```

Your completion percentage should be 7%. If not, troubleshoot to correct any errors.

## Task 2: 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.

Your completion percentage should be 20%. If not, troubleshoot to correct any errors.

## Task 3: Configure VTP and Security on the Switches

### Step 1. 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
```

### Step 2. Check the current VTP settings on the three switches.

Use the show vtp status command to determine the VTP operating mode for all three switches.

```
S1#show vtp status
VTP Version                : 2
Configuration Revision      : 0
Maximum VLANs supported locally : 64
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                  : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
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 : 64
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                  : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
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 : 64
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                  : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
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)
```

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. Note that all three switches are in server mode. Server mode is the default VTP mode for most Catalyst switches. In this activity, you will be using S1 as the VTP server, with S2 and S3 configured as VTP clients or in VTP transparent mode.

### Step 3. 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 4. Configure trunking and the native VLAN for the trunking ports on all three switches.**

On all switches, configure trunking and the native VLAN for FastEthernet interfaces 0/1-5. Only commands for fa0/1 on each switch are shown below.

```
S1(config)#interface fa0/1
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 99
S1(config-if)#no shutdown
S1(config-if)#interface fa0/2
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 99
S1(config-if)#no shutdown
S1(config-if)#end
```

```
S2(config)#interface fa0/1
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 99
S2(config-if)#no shutdown
S2(config-if)#end
```

```
S3(config)#interface fa0/2
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 99
S3(config-if)#no shutdown
S3(config-if)#end
```

**Step 5. 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 6. Configure VLANs on the VTP server.**

There are four VLANS required in this lab:

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

Configure these on the VTP server. Packet Tracer grading is case-sensitive.

```
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 7. 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, Fa0/3, 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

Are the same VLANs configured on all switches? \_\_\_\_\_

Why do S2 and S3 have different VLAN configurations at this point?

---

### Step 8. Create a new VLAN on S2 and S3.

```
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?

---

Delete VLAN 88 from S3.

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

### Step 9. Manually configure VLANs.

Configure the four VLANs identified in Step 6 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 10. 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? If not, troubleshoot the switch configurations and try again.

### Step 11. Assign switch ports to VLANs.

Refer to the port assignment table at the beginning of the activity to assign ports to the VLANs. 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 S3 switches should be similarly configured. Save the configuration when you are done.

```
S3(config)#interface range fa0/6 - fa0/10
S3(config-if-range)#switchport access vlan 30
S3(config-if-range)#interface range fa0/11 - fa0/17
S3(config-if-range)#switchport access vlan 10
S3(config-if-range)#interface range fa0/18 - fa0/24
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#
```

Your completion percentage should be 100%. Use the **Check Results** button to verify all components are complete.