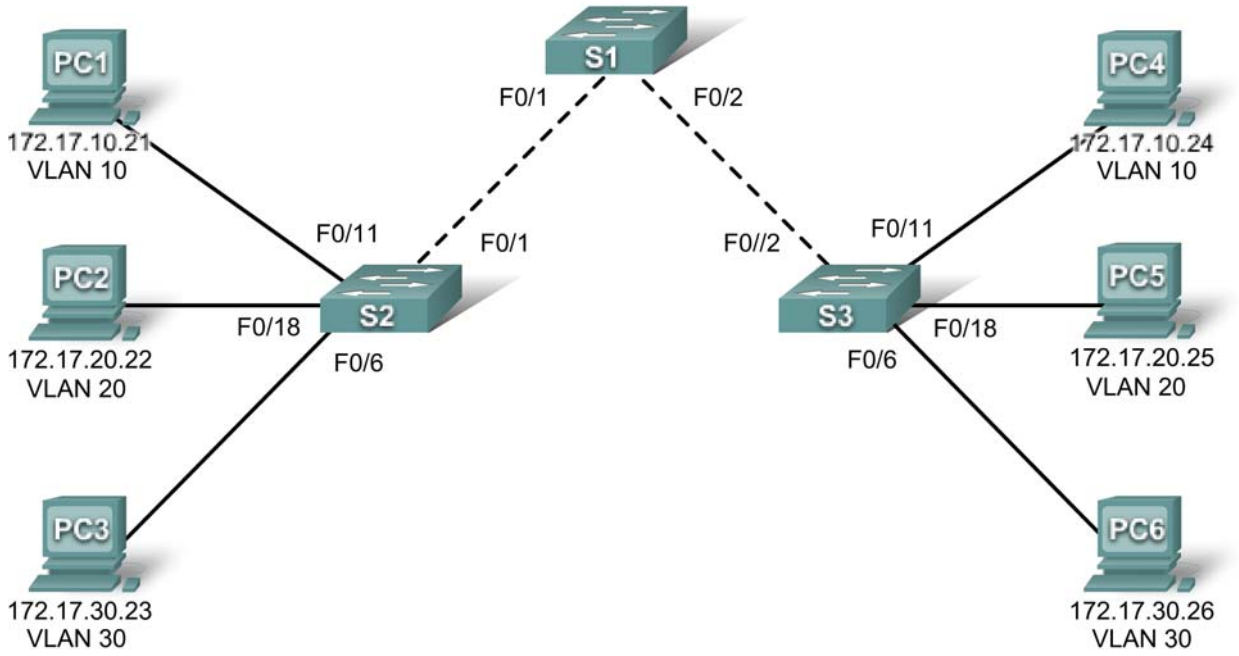
PT Activity 3.5.1: Basic VLAN Configuration

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 (Switches 2 and 3)

Ports	Assignment	Network
Fa0/1 – 0/5	VLAN 99 – Management&Native	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 configuration tasks on a switch
- Create VLANs
- Assign switch ports to a VLAN
- Add, move, and change ports
- Verify VLAN configuration
- Enable trunking on inter-switch connections
- Verify trunk configuration
- Save the VLAN configuration

Task 1: Perform Basic Switch Configurations

Perform Basic Switch Configurations. Packet Tracer will only grade switch hostnames.

- Configure the switch hostnames.
- 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 2: Configure and Activate Ethernet Interfaces

Configure the Ethernet interfaces of the six PCs with the IP addresses and default gateways from the addressing table.

Note: The IP address for PC1 will be marked as wrong for now. You will change the PC1 IP address later.

Task 3: Configure VLANs on the Switch

Step 1. Create VLANs on switch S1.

Use the **vlan** *vlan-id* command in global configuration mode to add VLANs to switch S1. There are four VLANs to configure for this activity. After you create the VLAN, you will be in vlan configuration mode, where you can assign a name to the VLAN with the **vlan** *name* command.

```
S1(config)#vlan 99
S1(config-vlan)#name Management&Native
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(Default)
S1(config-vlan)#exit
```

Step 2. Verify that the VLANs have been created on S1.

Use the **show vlan brief** command to verify that the VLANs have been created.

```
S1#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(Default)                    active
99   Management&Native                 active
```

Step 3. Configure and name VLANs on switches S2 and S3.

Create and name VLANs 10, 20, 30, and 99 on S2 and S3 using the commands from Step 1. Verify the correct configuration with the **show vlan brief** command.

What ports are currently assigned to the four VLANs you have created?

_____

Step 4. Assign switch ports to VLANs on S2 and S3.

Refer to the port assignment table. Ports are assigned to VLANs in interface configuration mode, using the **switchport access vlan** *vlan-id* command. Packet Tracer will only grade the first interface in each range (the interface the PC is connected to). Normally you would use the **interface range** command, but Packet Tracer does not support this command.

```
S2(config)#interface fastEthernet0/6
S2(config-if)#switchport access vlan 30
S2(config-if)#interface fastEthernet0/11
S2(config-if)#switchport access vlan 10
S2(config-if)#interface fastEthernet0/18
S2(config-if)#switchport access vlan 20
S2(config-if)#end
S2#copy running-config startup-config
Destination filename [startup-config]? [enter]
Building configuration...
[OK]
```

Note: The Fa0/11 access VLAN will be marked as wrong for now. You will correct this later in the activity.

Repeat the same commands on S3.

Step 5. Determine which ports have been added.

Use the **show vlan id** *vlan-number* command on S2 to see which ports are assigned to VLAN 10.

Which ports are assigned to VLAN 10? _____

Note: The **show vlan name** *vlan-name* displays the same output.

You can also view VLAN assignment information using the **show interfaces switchport** command.

Step 6. Assign the management VLAN.

A management VLAN is any VLAN that you configure to access the management capabilities of a switch. VLAN 1 serves as the management VLAN if you did not specifically define another VLAN. You assign the management VLAN an IP address and subnet mask. A switch can be managed via HTTP, Telnet, SSH, or SNMP. Because the out-of-the-box configuration of a Cisco switch has VLAN 1 as the default VLAN, VLAN 1 is a bad choice as the management VLAN. You do not want an arbitrary user who is connecting to a switch to default to the management VLAN. Recall that you configured the management VLAN as VLAN 99 earlier in this lab.

From interface configuration mode, use the **ip address** command to assign the management IP address to the 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
```

Assigning a management address allows IP communication between the switches, and also allows any host connected to a port assigned to VLAN 99 to connect to the switches. Because VLAN 99 is configured as the management VLAN, any ports assigned to this VLAN are considered management ports and should be secured to control which devices can connect to these ports.

Step 7. Configure trunking and the native VLAN for the trunking ports on all switches.

Trunks are connections between the switches that allow the switches to exchange information for all VLANS. By default, a trunk port belongs to all VLANs, as opposed to an access port, which can only belong to a single VLAN. If the switch supports both ISL and 802.1Q VLAN encapsulation, the trunks must specify which method is being used. Because the 2960 switch only supports 802.1Q trunking, it is not specified in this activity.

A native VLAN is assigned to an 802.1Q trunk port. In the topology, the native VLAN is VLAN 99. An 802.1Q trunk port supports traffic coming from many VLANs (tagged traffic) as well as traffic that does not come from a VLAN (untagged traffic). The 802.1Q trunk port places untagged traffic on the native VLAN. Untagged traffic is generated by a computer attached to a switch port that is configured with the native VLAN. One of the IEEE 802.1Q specifications for Native VLANs is to maintain backward compatibility with untagged traffic common to legacy LAN scenarios. For the purposes of this activity, a native VLAN serves as a common identifier on opposing ends of a trunk link. It is a best practice to use a VLAN other than VLAN 1 as the native VLAN.

```
S1(config)#interface fa0/1
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 99
S1(config-if)#interface fa0/2
```



```
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 99
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)#end

S3(config)#interface fa0/2
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 99
S3(config-if)#end
```

Verify that the trunks have been configured with the show interface trunk command.

```
S1#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99
Fa0/2       on           802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/2       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,30,99,1002,1003,1004,1005
Fa0/2       1,10,20,30,99,1002,1003,1004,1005

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,30,99,1002,1003,1004,1005
Fa0/2       1,10,20,30,99,1002,1003,1004,1005
```

Step 8. Verify that the switches can communicate.

From S1, ping the management address on both S2 and S3.

```
S1#ping 172.17.99.12
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.99.12, timeout is 2 seconds:
..!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/9 ms

S1#ping 172.17.99.13
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.99.13, timeout is 2 seconds:
..!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

Step 9. Ping several hosts from PC2.

Ping from host PC2 to host PC1 (172.17.10.21). Is the ping attempt successful? _____

Ping from host PC2 to the switch VLAN 99 IP address 172.17.99.12. Is the ping attempt successful?

_____

Because these hosts are on different subnets and in different VLANS, they cannot communicate without a Layer 3 device to route between the separate subnetworks.

Ping from host PC2 to host PC5. Is the ping attempt successful? _____

Because PC2 is in the same VLAN and the same subnet as PC5, the ping is successful.

Step 10. Move PC1 into the same VLAN as PC2.

The port connected to PC2 (S2 Fa0/18) is assigned to VLAN 20, and the port connected to PC1 (S2 Fa0/11) is assigned to VLAN 10. Reassign the S2 Fa0/11 port to VLAN 20. You do not need to first remove a port from a VLAN to change its VLAN membership. After you reassign a port to a new VLAN, that port is automatically removed from its previous VLAN.

```
S2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#interface fastethernet 0/11
S2(config-if)#switchport access vlan 20
S2(config-if)#end
```

Ping from host PC2 to host PC1. Is the ping attempt successful? _____

Step 11. Change the IP address and network on PC1.

Change the IP address on PC1 to 172.17.20.21. The subnet mask and default gateway can remain the same. Once again, ping from host PC2 to host PC1, using the newly assigned IP address.

Is the ping attempt successful? _____

Why was this attempt successful?

_____

_____

