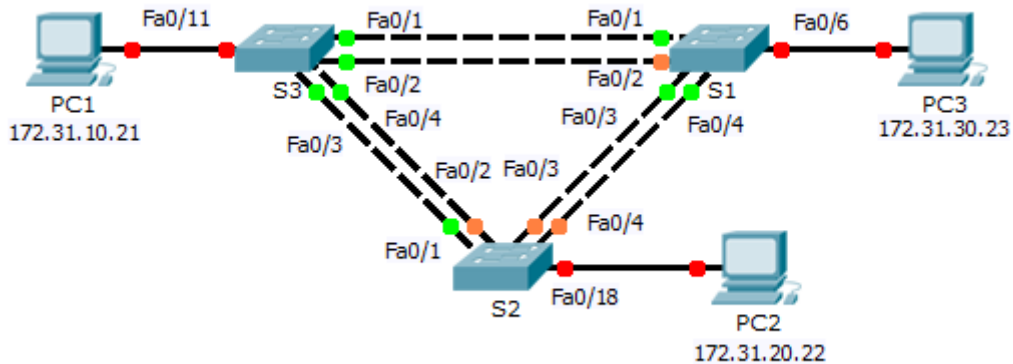


Packet Tracer – Configuring PVST+ Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 99	172.31.99.1	255.255.255.0	N/A
S2	VLAN 99	172.31.99.2	255.255.255.0	N/A
S3	VLAN 99	172.31.99.3	255.255.255.0	N/A
PC1	NIC	172.31.10.21	255.255.255.0	172.31.10.254
PC2	NIC	172.31.20.22	255.255.255.0	172.31.20.254
PC3	NIC	172.31.30.23	255.255.255.0	172.31.30.254

Switch Port Assignment Specifications

Ports	Assignments	Network
S1 F0/6	VLAN 30	172.17.30.0/24
S2 F0/18	VLAN 20	172.17.20.0/24
S3 F0/11	VLAN 10	172.17.10.0/24

Objectives

Part 1: Configure VLANs

Part 2: Configure Spanning Tree PVST+ and Load Balancing

Part 3: Configure PortFast and BPDU Guard

Background

In this activity, you will configure VLANs and trunks, and examine and configure the Spanning Tree Protocol primary and secondary root bridges. You will also optimize the switched topology using PVST+, PortFast, and BPDU guard.

Part 1: Configure VLANs

Step 1: Enable the user ports on S1, S2, and S3 in access mode.

Refer to the topology diagram to determine which switch ports (**S1**, **S2**, and **S3**) are activated for end-user device access. These three ports will be configured for access mode and enabled with the **no shutdown** command.

```
S1(config)# interface f0/6
S1(config-if)# switchport mode access
S1(config-if)# no shutdown
```

```
S2(config)# interface f0/18
S2(config-if)# switchport mode access
S2(config-if)# no shutdown
```

```
S3(config)# interface f0/11
S3(config-if)# switchport mode access
S3(config-if)# no shutdown
```

Step 2: Create VLANs.

Using the appropriate command, create VLANs 10, 20, 30, 40, 50, 60, 70, 80, and 99 on all of the switches.

```
S1(config)# vlan 10
S1(config-vlan)# vlan 20
S1(config-vlan)# vlan 30
S1(config-vlan)# vlan 40
S1(config-vlan)# vlan 50
S1(config-vlan)# vlan 60
S1(config-vlan)# vlan 70
S1(config-vlan)# vlan 80
S1(config-vlan)# vlan 99
```

```
S2(config)# vlan 10
S2(config-vlan)# vlan 20
S2(config-vlan)# vlan 30
S2(config-vlan)# vlan 40
S2(config-vlan)# vlan 50
S2(config-vlan)# vlan 60
S2(config-vlan)# vlan 70
S2(config-vlan)# vlan 80
S2(config-vlan)# vlan 99
```

```
S3(config)# vlan 10
S3(config-vlan)# vlan 20
S3(config-vlan)# vlan 30
S3(config-vlan)# vlan 40
```

```
S3(config-vlan)# vlan 50
S3(config-vlan)# vlan 60
S3(config-vlan)# vlan 70
S3(config-vlan)# vlan 80
S3(config-vlan)# vlan 99
```

Step 3: Assign VLANs to switch ports.

Port assignments are listed in the table at the beginning of the activity. Save your configurations after assigning switch ports to the VLANs.

```
S1(config)# interface f0/6
S1(config-if)# switchport access vlan 30

S2(config)# interface f0/18
S2(config-if)# switchport access vlan 20

S3(config)# interface f0/11
S3(config-if)# switchport access vlan 10
```

Step 4: Verify the VLANs.

Use the **show vlan brief** command on all switches to verify that all VLANs are registered in the VLAN table.

Step 5: Assign the trunks to native VLAN 99.

Use the appropriate command to configure ports F0/1 to F0/4 on each switch as trunk ports, and assign these trunk ports to native VLAN 99.

```
S1(config)# interface range f0/1-4
S1(config-if-range)# switchport mode trunk
S1(config-if-range)# switchport trunk native vlan 99

S2(config)# interface range f0/1-4
S2(config-if-range)# switchport mode trunk
S2(config-if-range)# switchport trunk native vlan 99

S3(config)# interface range f0/1-4
S3(config-if-range)# switchport mode trunk
S3(config-if-range)# switchport trunk native vlan 99
```

Step 6: Configure the management interface on all three switches with an address.

```
S1(config)# interface vlan99
S1(config-if)# ip address 172.31.99.1 255.255.255.0

S2(config)# interface vlan99
S2(config-if)# ip address 172.31.99.2 255.255.255.0

S3(config)# interface vlan99
S3(config-if)# ip address 172.31.99.3 255.255.255.0
```

Verify that the switches are correctly configured by pinging between them.

Part 2: Configure Spanning Tree PVST+ and Load Balancing

Because there is a separate instance of the spanning tree for every active VLAN, a separate root election is conducted for each instance. If the default switch priorities are used in root selection, the same root is elected for every spanning tree instance, as we have seen. This could lead to an inferior design. Some reasons to control the selection of the root switch include:

- The root switch is responsible for generating BPDUs for STP 802.1D and is the focal point for spanning tree to control traffic. The root switch must be capable of handling this additional load.
- The placement of the root defines the active switched paths in the network. Random placement is likely to lead to suboptimal paths. Ideally the root is in the distribution layer.
- Consider the topology used in this activity. Of the six trunks configured, only three are carrying traffic. While this prevents loops, it is a waste of resources. Because the root can be defined on the basis of the VLAN, you can have some ports blocking for one VLAN and forwarding for another. This is demonstrated below.

Step 1: Configure STP mode.

Use the **spanning-tree mode** command to configure the switches so they use PVST as the STP mode.

```
S1(config)# spanning-tree mode pvst
```

```
S2(config)# spanning-tree mode pvst
```

```
S3(config)# spanning-tree mode pvst
```

Step 2: Configure Spanning Tree PVST+ load balancing.

- a. Configure **S1** to be the primary root for VLANs 1, 10, 30, 50, and 70. Configure **S3** to be the primary root for VLANs 20, 40, 60, 80, and 99. Configure **S2** to be the secondary root for all VLANs.

```
S1(config)# spanning-tree vlan 1,10,30,50,70 root primary
```

```
S2(config)# spanning-tree vlan 1,10,20,30,40,50,60,70,80,99 root secondary
```

```
S3(config)# spanning-tree vlan 20,40,60,80,99 root primary
```

- b. Verify your configurations using the **show spanning-tree** command.

Part 3: Configure PortFast and BPDU Guard

Step 1: Configure PortFast on the switches.

PortFast causes a port to enter the forwarding state almost immediately by dramatically decreasing the time of the listening and learning states. PortFast minimizes the time it takes for the server or workstation to come online. Configure PortFast on the switch interfaces that are connected to PCs.

```
S1(config)# interface f0/6
```

```
S1(config-if-range)# spanning-tree portfast
```

```
S2(config)# interface f0/18
```

```
S2(config-if-range)# spanning-tree portfast
```

```
S3(config)# interface f0/11
```

```
S3(config-if-range)# spanning-tree portfast
```

Step 2: Configure BPDU guard on the switches.

The STP PortFast BPDU guard enhancement allows network designers to enforce the STP domain borders and keep the active topology predictable. The devices behind the ports that have STP PortFast enabled are unable to influence the STP topology. At the reception of BPDUs, the BPDU guard operation disables the port that has PortFast configured. The BPDU guard transitions the port into the err-disable state, and a message appears on the console. Configure BPDU guard on switch interfaces that are connected to PCs.

```
S1(config)# interface f0/6
```

```
S1(config-if)# spanning-tree bpduguard enable
```

```
S2(config)# interface f0/18
```

```
S2(config-if)# spanning-tree bpduguard enable
```

```
S3(config)# interface f0/11
```

```
S3(config-if)# spanning-tree bpduguard enable
```

Step 3: Verify your configuration.

Use the **show running-configuration** command to verify your configuration.