# Lab – Configuring Rapid PVST+, PortFast, and BPDU Guard
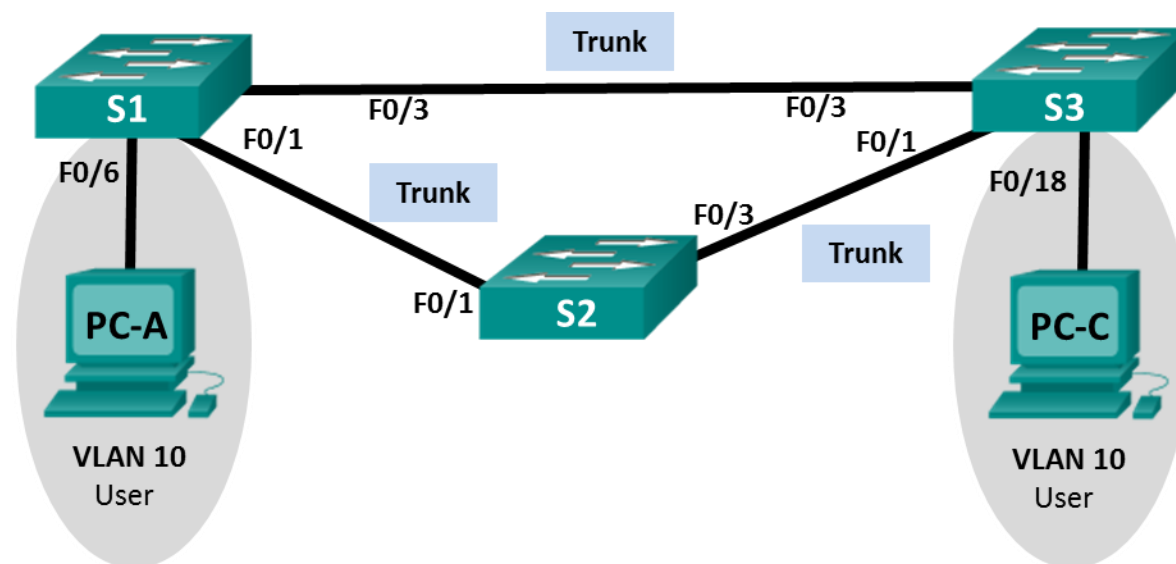
## Topology



## Addressing Table

| Device | Interface | IP Address | Subnet Mask |
|--------|-----------|------------|-------------|
| S1 | VLAN 99 | 192.168.1.11 | 255.255.255.0 |
| S2 | VLAN 99 | 192.168.1.12 | 255.255.255.0 |
| S3 | VLAN 99 | 192.168.1.13 | 255.255.255.0 |
| PC-A | NIC | 192.168.0.2 | 255.255.255.0 |
| PC-C | NIC | 192.168.0.3 | 255.255.255.0 |

## VLAN Assignments

| VLAN | Name |
|------|------|
| 10 | User |
| 99 | Management |

## Objectives

**Part 1: Build the Network and Configure Basic Device Settings**

**Part 2: Configure VLANs, Native VLAN, and Trunks**

**Part 3: Configure the Root Bridge and Examine PVST+ Convergence**

**Part 4: Configure Rapid PVST+, PortFast, BPDU Guard, and Examine Convergence**

## Background / Scenario

The Per-VLAN Spanning Tree (PVST) protocol is Cisco proprietary. Cisco switches default to PVST. Rapid PVST+ (IEEE 802.1w) is an enhanced version of PVST+ and allows for faster spanning-tree calculations and convergence in response to Layer 2 topology changes. Rapid PVST+ defines three port states: discarding, learning, and forwarding, and provides multiple enhancements to optimize network performance.

In this lab, you will configure the primary and secondary root bridge, examine PVST+ convergence, configure Rapid PVST+ and compare its convergence to PVST+. In addition, you will configure edge ports to transition immediately to a forwarding state using PortFast and prevent the edge ports from forwarding BDPUs using BDPU guard.

**Note**: This lab provides minimal assistance with the actual commands necessary for configuration. However, the required commands are provided in Appendix A. Test your knowledge by trying to configure the devices without referring to the appendix.

**Note**: The switches used with CCNA hands-on labs are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs.

**Note**: Make sure that the switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

## Required Resources

- 3 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

# Part 1:  Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings, such as the interface IP addresses, device access, and passwords.

**Step 1:   Cable the network as shown in the topology.**

**Step 2:   Configure PC hosts.**

**Step 3:   Initialize and reload the switches as necessary.**

**Step 4:   Configure basic settings for each switch.**

a.  Disable DNS lookup.

b.  Configure the device name as shown in the Topology.

c.  Assign **cisco** as the console and vty passwords and enable login.

d.  Assign **class** as the encrypted privileged EXEC mode password.

e.  Configure **logging synchronous** to prevent console messages from interrupting command entry.

f.  Shut down all switch ports.

g.  Copy the running configuration to startup configuration.

# Part 2:  Configure VLANs, Native VLAN, and Trunks

In Part 2, you will create VLANs, assign switch ports to VLANs, configure trunk ports, and change the native VLAN for all switches.

**Note**: The required commands for Part 2 are provided in Appendix A. Test your knowledge by trying to configure the VLANs, native VLAN, and trunks without referring to the appendix.

### Step 1:  Create VLANs.

Use the appropriate commands to create VLANs 10 and 99 on all of the switches. Name VLAN 10 as **User** and VLAN 99 as **Management**.

```
S1(config)# vlan 10
S1(config-vlan)# name User
S1(config-vlan)# vlan 99
S1(config-vlan)# name Management

S2(config)# vlan 10
S2(config-vlan)# name User
S2(config-vlan)# vlan 99
S2(config-vlan)# name Management

S3(config)# vlan 10
S3(config-vlan)# name User
S3(config-vlan)# vlan 99
S3(config-vlan)# name Management
```

### Step 2:  Enable user ports in access mode and assign VLANs.

For S1 F0/6 and S3 F0/18, enable the ports, configure them as access ports, and assign them to VLAN 10.

### Step 3:  Configure trunk ports and assign to native VLAN 99.

For ports F0/1 and F0/3 on all switches, enable the ports, configure them as trunk ports, and assign them to native VLAN 99.

### Step 4:  Configure the management interface on all switches.

Using the Addressing Table, configure the management interface on all switches with the appropriate IP address.

### Step 5:  Verify configurations and connectivity.

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

Use the **show interfaces trunk** command on all switches to verify trunk interfaces.

Use the **show running-config** command on all switches to verify all other configurations.

What is the default setting for spanning-tree mode on Cisco switches?


Verify connectivity between PC-A and PC-C. Was your ping successful?

If your ping was unsuccessful, troubleshoot the configurations until the issue is resolved.

**Note**: It may be necessary to disable the PC firewall to successfully ping between PCs.

# Part 3: Configure the Root Bridge and Examine PVST+ Convergence

In Part 3, you will determine the default root in the network, assign the primary and secondary root, and use the **debug** command to examine convergence of PVST+.

**Note**: The required commands for Part 3 are provided in Appendix A. Test your knowledge by trying to configure the root bridge without referring to the appendix.

### Step 1: Determine the current root bridge.

Which command allows a user to determine the spanning-tree status of a Cisco Catalyst switch for all VLANs? Write the command in the space provided.

Use the command on all three switches to determine the answers to the following questions:

**Note**: There are three instances of the spanning tree on each switch. The default STP configuration on Cisco switches is PVST+, which creates a separate spanning tree instance for each VLAN (VLAN 1 and any user-configured VLANs).

What is the bridge priority of switch S1 for VLAN 1?

What is the bridge priority of switch S2 for VLAN 1?

What is the bridge priority of switch S3 for VLAN 1?

Which switch is the root bridge?

Why was this switch elected as the root bridge?

### Step 2: Configure a primary and secondary root bridge for all existing VLANs.

Having a root bridge (switch) elected by MAC address may lead to a suboptimal configuration. In this lab, you will configure switch S2 as the root bridge and S1 as the secondary root bridge.

a. Configure switch S2 to be the primary root bridge for all existing VLANs. Write the command in the space provided.

b. Configure switch S1 to be the secondary root bridge for all existing VLANs. Write the command in the space provided.

Use the **show spanning-tree** command to answer the following questions:

What is the bridge priority of S1 for VLAN 1?

What is the bridge priority of S2 for VLAN 1?

Which interface in the network is in a blocking state?

### Step 3: Change the Layer 2 topology and examine convergence.

To examine PVST+ convergence, you will create a Layer 2 topology change while using the **debug** command to monitor spanning-tree events.

a. Enter the **debug spanning-tree events** command in privileged EXEC mode on switch S3.

---

```
S3# debug spanning-tree events
Spanning Tree event debugging is on
```

b.  Create a topology change by disabling interface F0/1 on S3.

```
S3(config)# interface f0/1
S3(config-if)# shutdown
*Mar  1 00:58:56.225: STP: VLAN0001 new root port Fa0/3, cost 38
*Mar  1 00:58:56.225: STP: VLAN0001 Fa0/3 -> listening
*Mar  1 00:58:56.225: STP[1]: Generating TC trap for port FastEthernet0/1
*Mar  1 00:58:56.225: STP: VLAN0010 new root port Fa0/3, cost 38
*Mar  1 00:58:56.225: STP: VLAN0010 Fa0/3 -> listening
*Mar  1 00:58:56.225: STP[10]: Generating TC trap for port FastEthernet0/1
*Mar  1 00:58:56.225: STP: VLAN0099 new root port Fa0/3, cost 38
*Mar  1 00:58:56.225: STP: VLAN0099 Fa0/3 -> listening
*Mar  1 00:58:56.225: STP[99]: Generating TC trap for port FastEthernet0/1
*Mar  1 00:58:56.242: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to down
*Mar  1 00:58:56.242: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed
state to down
*Mar  1 00:58:58.214: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to
administratively down
*Mar  1 00:58:58.230: STP: VLAN0001 sent Topology Change Notice on Fa0/3
*Mar  1 00:58:58.230: STP: VLAN0010 sent Topology Change Notice on Fa0/3
*Mar  1 00:58:58.230: STP: VLAN0099 sent Topology Change Notice on Fa0/3
*Mar  1 00:58:59.220: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down
*Mar  1 00:59:11.233: STP: VLAN0001 Fa0/3 -> learning
*Mar  1 00:59:11.233: STP: VLAN0010 Fa0/3 -> learning
*Mar  1 00:59:11.233: STP: VLAN0099 Fa0/3 -> learning
*Mar  1 00:59:26.240: STP[1]: Generating TC trap for port FastEthernet0/3
*Mar  1 00:59:26.240: STP: VLAN0001 Fa0/3 -> forwarding
*Mar  1 00:59:26.240: STP[10]: Generating TC trap for port FastEthernet0/3
*Mar  1 00:59:26.240: STP: VLAN0010 sent Topology Change Notice on Fa0/3
*Mar  1 00:59:26.240: STP: VLAN0010 Fa0/3 -> forwarding
*Mar  1 00:59:26.240: STP[99]: Generating TC trap for port FastEthernet0/3
*Mar  1 00:59:26.240: STP: VLAN0099 Fa0/3 -> forwarding
*Mar  1 00:59:26.248: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to up
*Mar  1 00:59:26.248: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed
state to up
```

**Note**: Before proceeding, use the **debug** output to verify that all VLANs on F0/3 have reached a forwarding state then use the command **no debug spanning-tree events** to stop the **debug** output.

Through which port states do each VLAN on F0/3 proceed during network convergence?


Using the time stamp from the first and last STP debug message, calculate the time (to the nearest second) that it took for the network to converge. **Hint**: The debug timestamp format is date hh.mm.ss:msec.

# Part 4: Configure Rapid PVST+, PortFast, BPDU Guard, and Examine Convergence

In Part 4, you will configure Rapid PVST+ on all switches. You will configure PortFast and BPDU guard on all access ports, and then use the **debug** command to examine Rapid PVST+ convergence.

**Note**: The required commands for Part 4 are provided in Appendix A. Test your knowledge by trying to configure the Rapid PVST+, PortFast, and BPDU guard without referring to the appendix.

### Step 1: Configure Rapid PVST+.

a. Configure S1 for Rapid PVST+. Write the command in the space provided.

b. Configure S2 and S3 for Rapid PVST+.

c. Verify configurations with the **show running-config | include spanning-tree mode** command.

```
S1# show running-config | include spanning-tree mode
spanning-tree mode rapid-pvst

S2# show running-config | include spanning-tree mode
spanning-tree mode rapid-pvst

S3# show running-config | include spanning-tree mode
spanning-tree mode rapid-pvst
```

### Step 2: Configure PortFast and BPDU Guard on access ports.

PortFast is a feature of spanning tree that transitions a port immediately to a forwarding state as soon as it is turned on. This is useful in connecting hosts so that they can start communicating on the VLAN instantly, rather than waiting on spanning tree. To prevent ports that are configured with PortFast from forwarding BPDUs, which could change the spanning tree topology, BPDU guard can be enabled. At the receipt of a BPDU, BPDU guard disables a port configured with PortFast.

a. Configure interface F0/6 on S1 with PortFast. Write the command in the space provided.

b. Configure interface F0/6 on S1 with BPDU guard. Write the command in the space provided.

c. Globally configure all non-trunking ports on switch S3 with PortFast. Write the command in the space provided.

d. Globally configure all non-trunking PortFast ports on switch S3 with BPDU guard. Write the command in the space provided.
 // Ik dacht spanning-tree portfast bpduguard default. Maar blijkbaar klopt da nie

### Step 3:  Examine Rapid PVST+ convergence.

a.  Enter the **debug spanning-tree events** command in privileged EXEC mode on switch S3.

b.  Create a topology change by enabling interface F0/1 on switch S3.

```
S3(config)# interface f0/1
S3(config-if)# no shutdown
*Mar  1 01:28:34.946: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 01:28:37.588: RSTP(1): initializing port Fa0/1
*Mar  1 01:28:37.588: RSTP(1): Fa0/1 is now designated
*Mar  1 01:28:37.588: RSTP(10): initializing port Fa0/1
*Mar  1 01:28:37.588: RSTP(10): Fa0/1 is now designated
*Mar  1 01:28:37.588: RSTP(99): initializing port Fa0/1
*Mar  1 01:28:37.588: RSTP(99): Fa0/1 is now designated
*Mar  1 01:28:37.597: RSTP(1): transmitting a proposal on Fa0/1
*Mar  1 01:28:37.597: RSTP(10): transmitting a proposal on Fa0/1
*Mar  1 01:28:37.597: RSTP(99): transmitting a proposal on Fa0/1
*Mar  1 01:28:37.597: RSTP(1): updt roles, received superior bpdu on Fa0/1
*Mar  1 01:28:37.597: RSTP(1): Fa0/1 is now root port
*Mar  1 01:28:37.597: RSTP(1): Fa0/3 blocked by re-root
*Mar  1 01:28:37.597: RSTP(1): synced Fa0/1
*Mar  1 01:28:37.597: RSTP(1): Fa0/3 is now alternate
*Mar  1 01:28:37.597: RSTP(10): updt roles, received superior bpdu on Fa0/1
*Mar  1 01:28:37.597: RSTP(10): Fa0/1 is now root port
*Mar  1 01:28:37.597: RSTP(10): Fa0/3 blocked by re-root
*Mar  1 01:28:37.597: RSTP(10): synced Fa0/1
*Mar  1 01:28:37.597: RSTP(10): Fa0/3 is now alternate
*Mar  1 01:28:37.597: RSTP(99): updt roles, received superior bpdu on Fa0/1
*Mar  1 01:28:37.605: RSTP(99): Fa0/1 is now root port
*Mar  1 01:28:37.605: RSTP(99): Fa0/3 blocked by re-root
*Mar  1 01:28:37.605: RSTP(99): synced Fa0/1
*Mar  1 01:28:37.605: RSTP(99): Fa0/3 is now alternate
*Mar  1 01:28:37.605: STP[1]: Generating TC trap for port FastEthernet0/1
*Mar  1 01:28:37.605: STP[10]: Generating TC trap for port FastEthernet0/1
*Mar  1 01:28:37.605: STP[99]: Generating TC trap for port FastEthernet0/1
*Mar  1 01:28:37.622: RSTP(1): transmitting an agreement on Fa0/1 as a response to a
proposal
*Mar  1 01:28:37.622: RSTP(10): transmitting an agreement on Fa0/1 as a response to a
proposal
*Mar  1 01:28:37.622: RSTP(99): transmitting an agreement on Fa0/1 as a response to a
proposal
*Mar  1 01:28:38.595: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
```

Using the time stamp from the first and last RSTP debug message, calculate the time that it took for the network to converge.

## Reflection

1. What is the main benefit of using Rapid PVST+?


2. How does configuring a port with PortFast allow for faster convergence?



3. What protection does BPDU guard provide?



## Appendix A – Switch Configuration Commands

## Switch S1

```
S1(config)# vlan 10
S1(config-vlan)# name User
S1(config-vlan)# vlan 99
S1(config-vlan)# name Management
S1(config-vlan)# exit
S1(config)# interface f0/6
S1(config-if)# no shutdown
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
S1(config-if)# interface f0/1
S1(config-if)# no shutdown
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# interface f0/3
S1(config-if)# no shutdown
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# interface vlan 99
S1(config-if)# ip address 192.168.1.11 255.255.255.0
S1(config-if)# exit
S1(config)# spanning-tree vlan 1,10,99 root secondary
S1(config)# spanning-tree mode rapid-pvst
S1(config)# interface f0/6
S1(config-if)# spanning-tree portfast
S1(config-if)# spanning-tree bpduguard enable
```

## Switch S2

```
S2(config)# vlan 10
S2(config-vlan)# name User
S2(config-vlan)# vlan 99
```

```
S2(config-vlan)# name Management
S2(config-vlan)# exit
S2(config)# interface f0/1
S2(config-if)# no shutdown
S2(config-if)# switchport mode trunk
S2(config-if)# switchport trunk native vlan 99
S2(config-if)# interface f0/3
S2(config-if)# no shutdown
S2(config-if)# switchport mode trunk
S2(config-if)# switchport trunk native vlan 99
S2(config-if)# interface vlan 99
S2(config-if)# ip address 192.168.1.12 255.255.255.0
S2(config-if)# exit
S2(config)# spanning-tree vlan 1,10,99 root primary
S2(config)# spanning-tree mode rapid-pvst
```

## Switch S3

```
S3(config)# vlan 10
S3(config-vlan)# name User
S3(config-vlan)# vlan 99
S3(config-vlan)# name Management
S3(config-vlan)# exit
S3(config)# interface f0/18
S3(config-if)# no shutdown
S3(config-if)# switchport mode access
S3(config-if)# switchport access vlan 10
S3(config-if)# spanning-tree portfast
S3(config-if)# spanning-tree bpduguard enable
S3(config-if)# interface f0/1
S3(config-if)# no shutdown
S3(config-if)# switchport mode trunk
S3(config-if)# switchport trunk native vlan 99
S3(config-if)# interface f0/3
S3(config-if)# no shutdown
S3(config-if)# switchport mode trunk
S3(config-if)# switchport trunk native vlan 99
S3(config-if)# interface vlan 99
S3(config-if)# ip address 192.168.1.13 255.255.255.0
S3(config-if)# exit
S3(config)# spanning-tree mode rapid-pvst
```