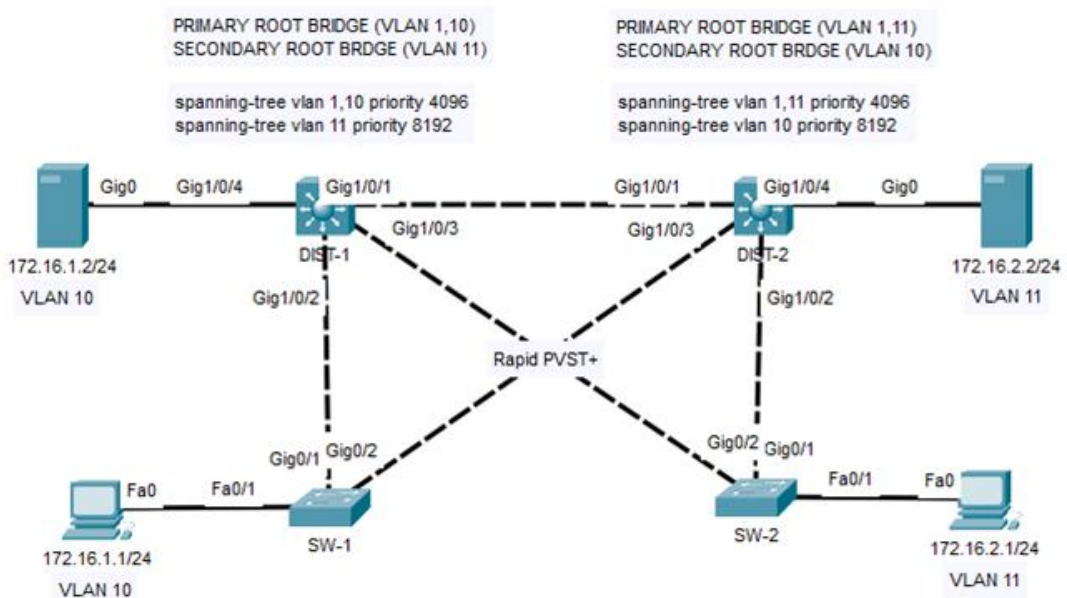


Root Guard

Lab Summary

Configure primary and secondary root bridge for VLAN 10 and VLAN 11 to enable redundancy. Configure Root guard on root bridge ports to prevent alternative root switch election. Verify spanning-tree configuration and root guard operation.

Figure 1 Lab Topology



Lab Configuration

Start Packet Tracer File: **root_guard.pkt**

Click on *DIST-1* switch and select the *CLI* folder.

Step 1: Enter global configuration mode.

```
DIST-1>enable  
DIST-1#configure terminal
```

Step 2: Create VLAN 10 and VLAN 11 on DIST-1 switch.

```
DIST-1(config)#vlan 10  
DIST-1(config-vlan)#vlan 11  
DIST-1(config-vlan)#exit
```

Step 3: Enable Rapid PVST+ spanning tree protocol.

```
DIST-1(config)#spanning-tree mode rapid-pvst
```

Step 4: Configure interface Gi1/0/4 as an access port and assign VLAN 10.

```
DIST-1(config)#interface Gi1/0/4  
DIST-1(config-if)#switchport mode access  
DIST-1(config-if)#switchport access vlan 10
```

Step 5: Configure all switch uplinks as trunk ports to neighbors.

```
DIST-1(config)#interface Gi1/0/1  
DIST-1(config-if)#switchport mode trunk  
DIST-1(config)#interface Gi1/0/2  
DIST-1(config-if)#switchport mode trunk  
DIST-1(config-if)#interface Gi1/0/3  
DIST-1(config-if)#switchport mode trunk  
DIST-1(config-if)#exit
```

Step 6: Configure DIST-1 switch as primary root bridge for VLAN 10 and secondary root bridge for VLAN 11.

```
DIST-1(config)#spanning-tree vlan 1,10 priority 4096  
DIST-1(config)#spanning-tree vlan 11 priority 8192
```

Step 7: Configure Root guard on interface Gi1/0/2 and Gi1/0/3 trunk uplinks to access switches.

```
DIST-1(config)#interface Gi1/0/2  
DIST-1(config-if)#spanning-tree guard root  
DIST-1(config-if)#interface Gi1/0/3  
DIST-1(config-if)#spanning-tree guard root  
DIST-1(config-if)#end  
DIST-1#copy running-config startup-config
```

Click on *DIST-2* switch and select the *CLI* folder.

Step 8: Enter global configuration mode.

```
DIST-2>enable  
DIST-2#configure terminal
```

Step 9: Create VLAN 10 and VLAN 11 on DIST-2 switch.

```
DIST-2(config)#vlan 10  
DIST-2(config-vlan)#vlan 11  
DIST-2(config-vlan)#exit
```

Step 10: Enable Rapid PVST+ spanning tree protocol.

```
DIST-2(config)#spanning-tree mode rapid-pvst
```

Step 11: Configure interface Gi1/0/4 as an access port and assign VLAN 10.

```
DIST-2(config)#interface Gi1/0/4  
DIST-2(config-if)#switchport mode access  
DIST-2(config-if)#switchport access vlan 11
```

Step 12: Configure all switch uplinks as trunk ports to neighbors.

```
DIST-2(config)#interface Gi1/0/1  
DIST-2(config-if)#switchport mode trunk  
DIST-2(config)#interface Gi1/0/2  
DIST-2(config-if)#switchport mode trunk  
DIST-2(config-if)#interface Gi1/0/3  
DIST-2(config-if)#switchport mode trunk  
DIST-2(config-if)#exit
```

Step 13: Configure DIST-2 switch as primary root bridge for VLAN 11 and secondary root bridge for VLAN 10.

```
DIST-2(config)#spanning-tree vlan 1,11 priority 4096  
DIST-2(config)#spanning-tree vlan 10 priority 8192
```

Step 14: Configure Root guard on interface Gi1/0/2 and Gi1/0/3 trunk uplinks to access switches.

```
DIST-2(config)#interface Gi1/0/2  
DIST-2(config-if)#spanning-tree guard root  
DIST-2(config-if)#interface Gi1/0/3  
DIST-2(config-if)#spanning-tree guard root
```

Click on SW-1 switch and select the CLI folder.

Step 15: Enter global configuration mode.

```
SW-1>enable  
SW-1#configure terminal
```

Step 16: Enable Rapid PVST+ spanning tree protocol.

```
SW-1(config)#spanning-tree mode rapid-pvst
```

Click on SW-2 switch and select the *CLI* folder.

Step 17: Enter global configuration mode.

```
SW-2>enable
SW-2#configure terminal
```

Step 18: Enable Rapid PVST+ spanning tree protocol.

```
SW-2(config)#spanning-tree mode rapid-pvst
```

Verify Lab

Step 19: Verify that DIST-1 switch is currently the primary root bridge for VLAN 10.

```
DIST-1#show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority        4106
             Address        0001.648D.C554
             This bridge is the root
             Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

  Bridge ID  Priority        4106 (priority 4096 sys-id-ext 10)
             Address        0001.648D.C554
             Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
             Aging Time 20
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Gi1/0/3	Desg	FWD	4	128.3	P2p
Gi1/0/2	Desg	FWD	4	128.2	P2p
Gi1/0/4	Desg	FWD	4	128.4	P2p
Gi1/0/1	Desg	FWD	4	128.1	P2p

Step 20: Verify that DIST-2 switch is currently the primary root bridge for VLAN 11.

```
DIST-2#show spanning-tree vlan 11
VLAN0011
  Spanning tree enabled protocol rstp
  Root ID    Priority        4107
             Address        0003.E427.E259
             This bridge is the root
             Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

  Bridge ID  Priority        4107 (priority 4096 sys-id-ext 11)
```

Address 0003.E427.E259
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface	Role	Sts	Cost	Prio.Nbr	Type
Gi1/0/1	Desg	FWD	4	128.1	P2p
Gi1/0/4	Desg	FWD	4	128.4	P2p
Gi1/0/2	Desg	FWD	4	128.2	P2p
Gi1/0/3	Desg	FWD	4	128.3	P2p

Step 21: Verify there is L2 connectivity from host to server within VLAN 10.

C:\>**ping 172.16.1.2**

Pinging 172.16.1.2 with 32 bytes of data:

Reply from 172.16.1.2: bytes=32 time<1ms TTL=128

Reply from 172.16.1.2: bytes=32 time<1ms TTL=128

Reply from 172.16.1.2: bytes=32 time<1ms TTL=128

Reply from 172.16.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.1.2:

Packets: Sent = 4, Received = 4, Lost = 0 (**0% loss**)

Step 22: Configure SW-1 with priority zero (0) for VLAN 10 to simulate adding a root bridge to the switching domain.

SW-1(config)#**spanning-tree vlan 1,10 priority 0**

Step 23: Verify the system error message on DIST-1 and DIST-2 where interface Gi1/0/2 and Gi1/0/3 now root-inconsistent state and traffic is discarded.

DIST-1#%SPANTREE-2-ROOTGUARDBLOCK: Port **1/0/2** tried to become non-designated in VLAN 1.
Moved to root-inconsistent state

DIST-1#%SPANTREE-2-ROOTGUARDBLOCK: Port **1/0/2** tried to become non-designated in VLAN 10.
Moved to root-inconsistent state

DIST-2#%SPANTREE-2-ROOTGUARDBLOCK: Port **1/0/3** tried to become non-designated in VLAN 10.
Moved to root-inconsistent state

DIST-2#%SPANTREE-2-ROOTGUARDBLOCK: Port **1/0/3** tried to become non-designated in VLAN 1.
Moved to root-inconsistent state

Step 24: Verify there is NO L2 connectivity from host to server within VLAN 10.

C:\>**ping 172.16.1.2**

Pinging 172.16.1.2 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 172.16.1.2:

Packets: Sent = 4, Received = 0, Lost = 4 (**100% loss**)

Step 25: Remove spanning tree priority command on SW-1 to restore normal spanning-tree operation for VLAN 10.

SW-1(config)#**no spanning-tree vlan 1,10 priority 0**

Step 26: Verify that L2 connectivity is restored from host to server within VLAN 10.

C:\>**ping 172.16.1.2**

Pinging 172.16.1.2 with 32 bytes of data:

Reply from 172.16.1.2: bytes=32 time<1ms TTL=128

Reply from 172.16.1.2: bytes=32 time<1ms TTL=128

Reply from 172.16.1.2: bytes=32 time<1ms TTL=128

Reply from 172.16.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.1.2:

Packets: Sent = 4, Received = 4, Lost = 0 (**0% loss**)

Step 27: Perform shutdown on SW-1 interface Gi0/1 to test failover to secondary root bridge for VLAN 10 (DIST-2).

SW-1(config)#**interface Gi0/1**

SW-1(config-if)#**shut**

C:\>**ping 172.16.1.2**

Pinging 172.16.1.2 with 32 bytes of data:

Reply from 172.16.1.2: bytes=32 time<1ms TTL=128

Reply from 172.16.1.2: bytes=32 time<1ms TTL=128

Reply from 172.16.1.2: bytes=32 time=1ms TTL=128

Reply from 172.16.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.1.2:

Packets: Sent = 4, Received = 4, Lost = 0 (**0% loss**)

Lab Notes

Root guard is an STP enhancement that prevents a switch from becoming a root bridge. The **spanning-tree guard root** command is configured on all designated ports of a root bridge. That will cause the switch to transition a designated port to root-inconsistent state when a superior BPDU is received.

That would trigger STP election of a new root bridge. This could happen when a new switch with lower priority than the current root bridge is connected to a switching domain. Recovery is automatic and designated port transitions from discarding to forwarding when superior BPDUs are no longer received.

The recommended method for assigning primary and secondary root bridge to VLANs is with the priority command shown with this lab.

Typically you would assign zero (0) priority to a VLAN on the primary root bridge. This was not done with this lab since the rogue switch was assigned zero priority to VLAN 10 simulating a root bridge new election. VLAN priority must also be configured in increments of 4096 starting with zero.

There is an alternate method to priority that is not recommended since it is less deterministic. It does not specifically assign priority zero to the primary root bridge. Instead it only assigns a lower priority than existing switches. The result is that adding a new switch with a lower priority would change the root bridge selection.

```
switch(config)#spanning-tree vlan 1,10 root primary  
switch(config)#spanning-tree vlan 11 root secondary
```