Lab 4: Layer 2 Redundancy – Spanning Tree Protocol

Contents

Follow us:

Introduction to LAB 4

In this lab, you will see how spanning tree works by default (when you just enable it) and what you can do with additional modifications. You will have not only redundancy, but also load sharing.

Exercise 1: Spanning Tree Topology with a Single VLAN

Let's start with a simple topology with three switches. They will be connected to each other and the Spanning Tree Protocol will prevent Layer 2 loops between them

1. Create the topology

Move three switches (2960) to the topology, change their display names (from the config tab) to Switch1, Switch2 and Switch3 and connect them as per the picture below.
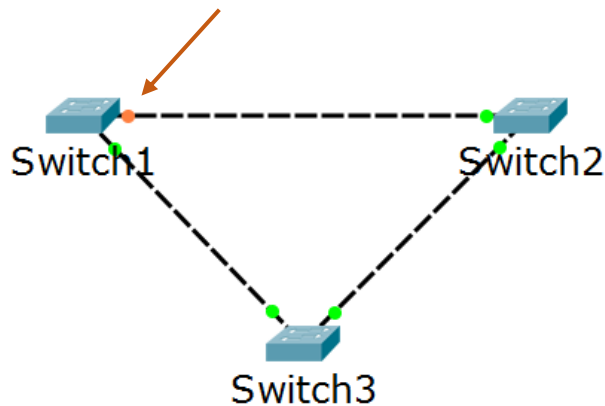
Note that this will create a loop and since spanning tree is enabled by default, it will take some time for it to calculate the topology and to allow all ports but one. Either wait (for about a minute) or click on <u>fast forward time</u> in the packet tracer's bottom menu. After this, you should see all ports except one in green and one port (pointed with the arrow) in a different color, indicating that it is blocked by STP. To see this clearly, you can temporarily hide the port names (as

---

this is done in the screenshot) from the Options -> Preferences -> Always Show Port Labels in Logical Workspace

2. Observe the default behavior and who will become the Root
    Open the CLI of each switch and:
    - Change the hostname to Switch1, Switch2 and Switch3 respectively, to represent the display names that you set up earlier
    - Type **show spanning-tree** and find the following information:
      - Which switch is the Root?
      - Which ports are root?
      - Which ports are designated?
      - Which port is blocking (alternate)?

In the case with the topology from the screenshot below, the Root is Switch3 and the port roles are as noted in the picture:
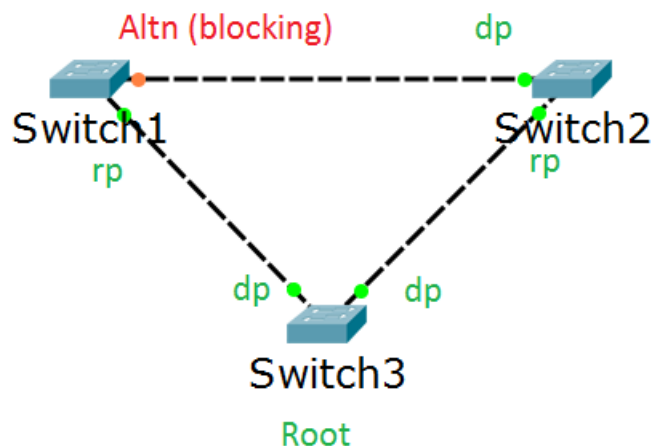
Where **dp** = designated port, **rp** = root port and **Altn** is the alternate, or blocking port. Explain why exactly these ports are taking these roles and why Switch3 is the Root.

Note: In your particular case, you may have another Root and different port roles. It depends on the BID (Bridge ID) values of your switches

3. Change the Root for VLAN 1

Go to the CLI of the switch which has the blocking port (in this case, Switch1) and make it the Root for VLAN 1. To force a switch to be a Root, you have to change its priority to a lower priority value than the other switches have.

To force Switch1 (again, this can be a different switch in your case) to become the Root, type the following from the global config mode:

spanning-tree vlan 1 priority 4096

4. Use **show spanning-tree** again to see the changes and to confirm that your Root now has changed. In this case, Switch one has become the new Root and its priority for VLAN1 is 4097 (4096 + 1 for VLAN1)
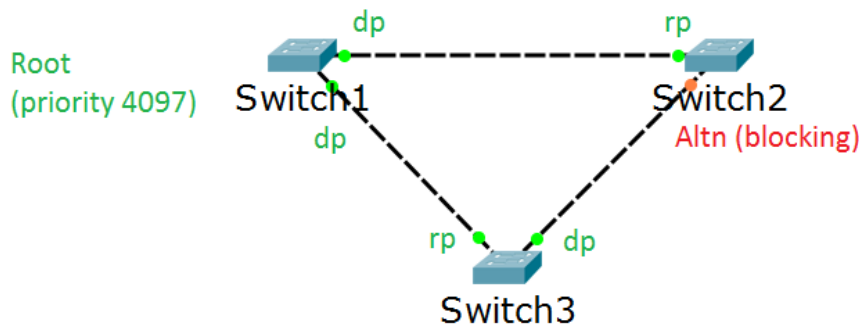
Exercise 2: PVST+ and Load Sharing with Multiple Root Switches

In this exercise, you will create two VLANs and each of them will have a client and a server assigned to it. The traffic will pass through a number of switches connected in a loop topology. Initially, spanning tree will prevent from loops and because of the trunks between the switches, each client will reach its server. However, the problem here is that spanning tree will select a single switch as a Root for all VLANs. This means that this switch can become overloaded while the other one will stay only as a backup, doing nothing during normal operations. To

change this, you will configure the Per-VLAN Spanning Tree Plus (PVST+) so the Root role will depend on the VLAN. The traffic from VLAN 5 will have one Root and the traffic from VLAN 6 will have another switch as a Root. This approach will provide load sharing in addition to the loop prevention benefit from spanning tree. Finally, note that whichever of the switches fails, the other one will be able to handle the traffic from both VLANs

1. Create the physical topology

Move the following devices in the topology:

- Four (2960) Switches
- Two Servers (the third icon from the list of End Devices)
- Two PCs (the first icon from the list of End Devices)

Then, rename the devices so their numbers start with 1 (not with 0) and connect them as per the picture below

Follow us:
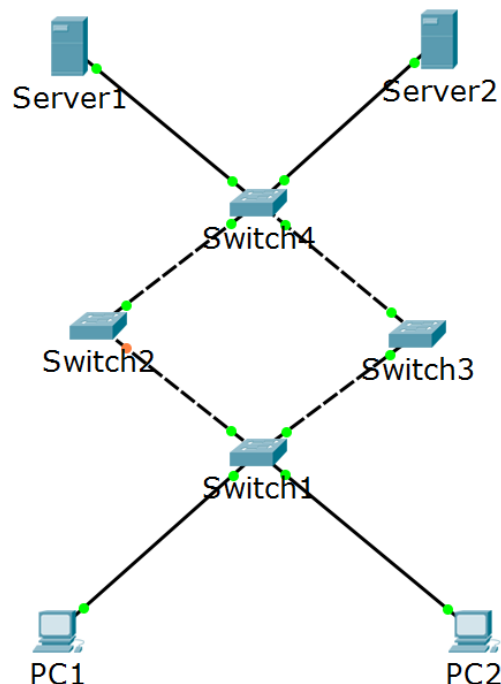
Note the ports which connects the switches to each other and the end devices to the switches. This may be different for each of your topologies. Also, remember that you can turn on and off displaying of the port names from <u>Options</u> -> <u>Preferences</u> -> <u>Always Show Port Labels in Logical Workspace</u>

2. Create two VLANs.

You will create VLAN 5 and VLAN 6 on the switches. PC1 will communicate with Server1 in VLAN 5 and PC2 will communicate with Server2 in VLAN6.

In each switch, from the global configuration mode, type:

- **vlan 5**
- **vlan 6**

While in the switch configuration, rename the switches (**hostname SwitchN**, where N is from 1 to 4, respectively)

3. Associate the access and trunk ports

Configure the ports which are connected to the end devices as access ports (untagged):

- Switch1 port which goes to PC1 should be access port in VLAN5
- Switch1 port which goes to PC2 should be access port in VLAN6
- Switch4 port which goes to Server1 should be access port in VLAN5
- Switch4 port which goes to Server2 should be access port in VLAN6
- All switch to switch ports should be trunk ports in VLAN5 and VLAN6

For the access ports configuration, use the following commands from the interface configuration mode:

- **switchport mode access**
- **switchport access vlan X** (where X is the VLAN number)

For the trunk ports configuration, use the following command from the interface configuration mode:

- **switchport mode trunk** (note that in Cisco, all VLANs are automatically allowed on the trunk)

---

4. Find who is the Root in your topology. To do this, type **show spanning-tree** on each switch. In this case, the Root is Switch3.

   Note the result from the **show spanning-tree** command – it should say <u>This bridge is the root</u> for VLAN1, VLAN5 and VLAN6.

5. Assign IP addresses for the end devices in VLAN5 and VLAN6 according to the table below

Device/Port	IP Address/Mask	Belongs to (informational only)
PC1/Fa0	10.5.5.1/24	Vlan 5
Server1/Fa0	10.5.5.100/24	Vlan 5
PC2/Fa0	10.6.6.1/24	Vlan 6
Server2/Fa0	10.6.6.100/24	Vlan 6

6. Test the connectivity in the VLANs.

   From PC1 ping Server1 (10.5.5.100) and from PC2 ping Server2 (10.6.6.100). Both pings should be successful.

7. Observe that the traffic from both VLANs (5 and 6) goes through a single device, your Root. This means that although you have connectivity for each PC to Server communication, you do <u>not</u> have load balancing.
   To examine this, you can do one or both of the following things:
   - Use the **show span** on the switch that has the blocking (alternate) port and see that it is blocked for <u>all</u> VLANs (1, 5 and 6)
   - Switch to Simulation mode in the packet tracer and monitor the path that each ICMP packet takes when you ping between the devices

   The following picture represents the idea. Note that Switch3 is the Root in this example (for all VLANs) and because of this, all traffic goes through it.
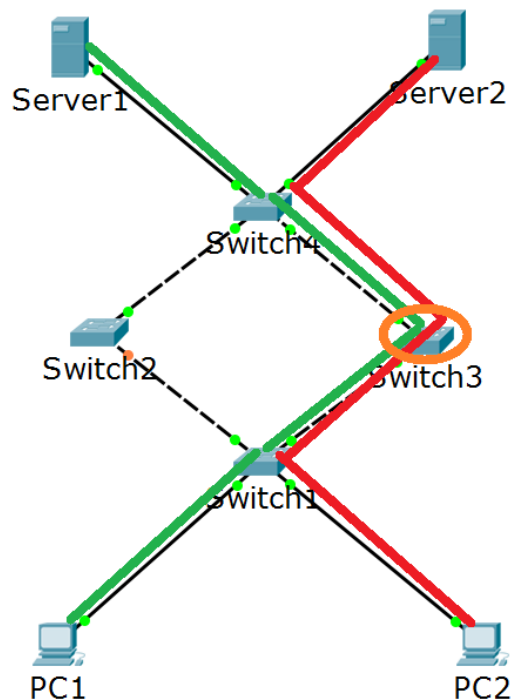
8. Implement load sharing with PVST+
    Now you will force the Root switch for VLAN5 to be Switch2 and the Root switch for VLAN6 to be Switch3
    Go to Switch2 and in the global config mode, type either:

    - **spanning-tree vlan 5 root primary**

    or

    - **spanning-tree vlan 5 priority N** (N is a number lower than 32768 and in increments of 4096. For example, type 4096)

    The first command sets the priority to 24581 (6x4096 + 5, the VLAN number) and the second one creates a specific priority number but in both case, this switch priority for VLAN5 will be lower than in the other three switches which have the default value. That is why it will become the Root for VLAN5.

    Then, go to Switch3 and in the global config mode, type the same command but this time use VLAN6:

- **spanning-tree vlan 6 root primary**

or

- **spanning-tree vlan 6 priority N** (N is a number lower than 32768 and in increments of 4096. For example, type 4096)

This will force Switch3 to be the Root for VLAN6.

9. Observe the behavior after the new configuration
You may need to allow up to a minute for the network to converge (to stabilize). Then, check the Root switches for VLAN5 and VLAN6. Again, to examine this, you can do one or both of the following things:
    - Use the **show span** on both switches (Switch2 and Switch3) and confirm that Switch2 is Root for VLAN5 and Switch3 is Root for VLAN6. Also, Switch2 has one blocked (alternate) port for VLAN6 and at the same time Switch3 has one blocked port for VLAN5
    - Switch to Simulation mode in the packet tracer and monitor the path that each ICMP packet takes

The following picture represents the idea. Note that because there are different Root switches for the different VLANs, the traffic from PC1 and PC2 takes different paths to reach its destination
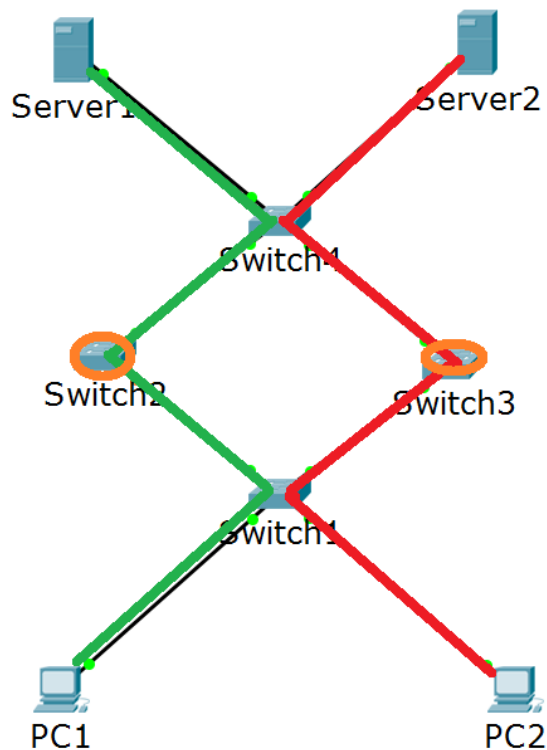
10. (optional) Save your LAB configuration and topology from the File -> Save As... menu in the packet tracer.
11. (optional) Test the failover. To do this, you have several options. First, select one switch (between Switch2 and Switch3) for which you will simulate a crash. Then, disable either the port which goes to Switch1 or the one which goes to Switch4 or both (with the **shutdown** command). Another option is to simply delete the whole switch from the topology. In either case, your pings between PC1 and Server1 and PC2 and Server2 should be again successful. This is because spanning tree will unblock all the ports which does not have alternate path to reach the destination

Note: You may need to wait for the failover and for the spanning tree to recalculate the topology, but the idea is that it should happen automatically.

You have completed LAB 4.