EXPERIMENT 3

Aim

Simulation of Spanning Tree Protocol (STP)

Prerequisite

Nil

Outcome

To impart knowledge of Computer Networking Technology

Theory

The Spanning Tree Protocol (STP) is a network protocol used in Ethernet networks to **prevent loops** in bridged or switched networks. Loops can cause **broadcast storms** and lead to network congestion and instability. STP accomplishes this by creating a **loop-free logical topology** within a network, ensuring that there is only **one active path** between any two devices in the network.

Here are some key concepts and theory about the Spanning Tree Protocol:

- **Loop Prevention**: STP ensures that Ethernet networks do not have redundant loops, preventing broadcast storms and network instability.
- **Root Bridge**: The Root Bridge is the central point in the network topology, serving as a reference for all other bridges to determine their paths.
- **Root Port**: Each non-Root Bridge selects a Root Port, which is the shortest path to the Root Bridge, ensuring efficient data forwarding.
- **Designated Ports**: Designated Ports are responsible for forwarding traffic within network segments, optimizing communication.
- **Blocked Ports**: STP places certain ports in a blocked state to break loops, temporarily preventing data flow through them.
- **BPDU**: Bridge Protocol Data Units (BPDUs) are exchanged between bridges to convey topology information, facilitating network stability.
- **STP States**: Ports transition through Blocking, Listening, Learning, and Forwarding states to establish a loop-free topology while reacting to topology changes.

STP is a crucial protocol for ensuring the stability and reliability of Ethernet networks, especially in environments where redundancy is required. By preventing loops and ensuring a single active path between devices, STP helps maintain network integrity and performance.

Procedure

1. **Set Up Physical Connections:**

   Connect the switches using Ethernet cables to create a network topology with redundant links, which can potentially form loops.

2. **Access Switches:**

   Use a computer with terminal software (e.g., PuTTY or Terminal) to access the command-line interface (CLI) of each switch. You may need the switch's console cable or access through SSH.

3. **Configure STP:**

   Enter the CLI of each switch.

   Enter global configuration mode by typing: **enable** or **configure terminal**.

4. **View STP Information:**

   Use the following command to view STP information: `show spanning-tree`

   Note the Root Bridge, Root Port, and Designated Ports for each switch.

5. **Introduce Changes:**

   Disconnect and reconnect Ethernet cables to simulate network changes. Observe how STP reacts to topology changes.

6. **Analyse Results:**

   Analyse the data obtained during the simulation, including the Root Bridge selection, port states, and convergence times.

Output

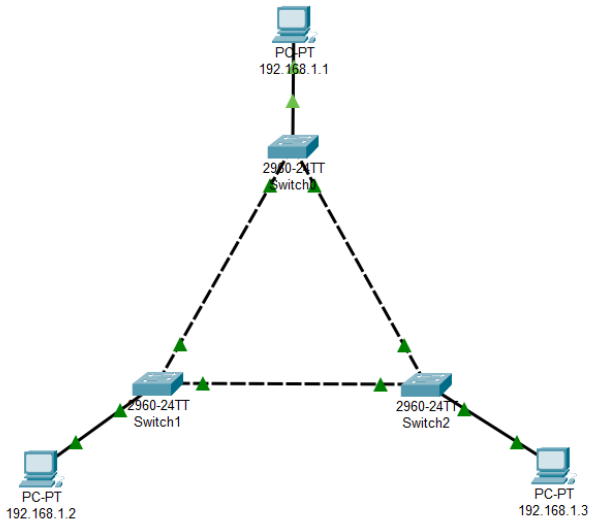

Figure 1: Without Spanning Tree

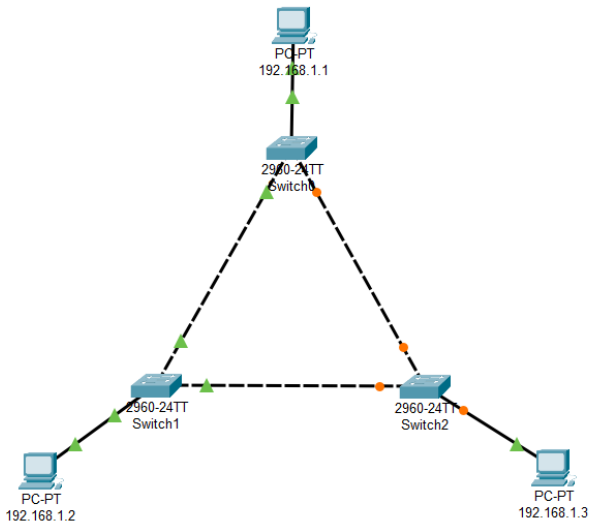

Figure 2: With Spanning Tree

```
Switch>
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#spanning-tree vlan 1
Switch(config)#^Z
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#wr
Building configuration...
[OK]
```

Figure 1: Enabling Spanning Tree

```
Switch#enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#no sp
Switch(config)#no spanning-tree
Switch(config)#no spanning-tree vlan 1
Switch(config)#^Z
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#wr
Building configuration...
[OK]
```

Figure 2: Disabling Spanning Tree

```
Switch#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0001.C9E2.C5E7
              Cost        19
              Port        2(FastEthernet0/2)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15
sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     000A.F32E.19B0
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15
sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- --------
--------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Root FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
```

Figure 5: Spanning Tree Details

Observation & Learning

Throughout the experiment, we observed that Spanning Tree Protocol (STP) played a pivotal role in preventing network loops by strategically blocking redundant connections while maintaining network stability. Notably, STP exhibited rapid adaptation to network changes, minimizing disruptions caused by topology modifications. The autonomous selection of a Root Bridge by STP influenced the network structure and dictated the behaviour of switch ports, ensuring a loop-free topology.

Understanding the various port states, including Blocking and Forwarding, was key to grasping how STP maintains network integrity. Overall, STP's significance in networks with multiple connections became evident as it effectively safeguarded against loops, promoted reliability, and showcased its ability to react swiftly to changes, reducing network downtime and enhancing overall network responsiveness.

Conclusion

In conclusion, the experiment demonstrated the effectiveness of the Spanning Tree Protocol in preventing network loops and maintaining a stable Ethernet network. STP successfully selected a Root Bridge and configured port states to ensure a loop-free topology. It reacted promptly to topology changes, which is essential for network reliability.

Questions

1. **What happens if STP is disabled on all the switches in the network?**

   Disabling STP on all switches in the network can lead to the **formation of network loops**. This can result in **broadcast storms**, **network congestion**, and **instability** due to redundant paths. It's essential to have STP enabled to prevent such issues.

2. **What is meant by Designated, Root, and Blocked Interfaces?**

   Designated Interface: These are ports on a switch that have been selected to forward traffic for a particular network segment. They are responsible for forwarding data within their respective segments.

   Root Interface: The Root Interface is the switch port that offers the shortest path to the Root Bridge. It is in the Forwarding state and serves as the best path to reach the Root Bridge.

   Blocked Interface: Blocked Interfaces are ports that are in a Blocking state. They do not forward data but exist to prevent loops by temporarily deactivating redundant paths.

3. **What are the different ways to identify the Root in the STP?**

   The Root Bridge in STP is identified based on the **Bridge ID**. The Bridge ID is composed of a **priority value** and a **MAC address**. The Root Bridge is the bridge with the **lowest Bridge ID**. If two bridges have the same priority, the one with the **lowest MAC address** becomes the Root Bridge. Additionally, you can use the `show spanning-tree` command on a switch to directly identify the Root Bridge in the output.