**Experiment-3**

**Part A**

**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 the network topology, which can cause broadcast storms and degrade network performance. STP was developed by Dr. Radia Perlman in 1985 and is defined by the IEEE 802.1D standard. There are also newer versions of STP, such as Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP), which offer faster convergence and more advanced features.

Here's how STP works:

* **Loop Prevention:** In a network with multiple interconnected switches, there is a potential for loops to occur, which can lead to broadcast storms and network instability. STP ensures that only one active path exists between any two network nodes by blocking redundant paths.
* **Bridge Election:** In STP, each switch in the network is assigned a Bridge ID (BID), which consists of a priority value and a unique MAC address. The switch with the lowest BID becomes the root bridge, which serves as the reference point for the STP calculations.
* **Path Cost Calculation:** STP calculates the cost of each path from non-root switches to the root bridge. The cost is based on the link speed (e.g., 100 Mbps, 1 Gbps) and is used to determine the best path to reach the root bridge.
* **Port States:** STP defines several port states, including Blocking, Listening, Learning, and Forwarding. Initially, all ports are in the Blocking state to prevent loops. Ports transition through these states as the STP algorithm determines the best path to the root bridge.
* **Convergence:** When a change occurs in the network, such as a link failure or a new switch being added, STP recalculates the topology to ensure that there are no loops. This process is called convergence, and it can take some time, depending on the STP version being used. RSTP is faster at converging than the original STP.
* **Loop-Free Topology:** Once STP convergence is complete, the network topology is loop-free, and data can flow between devices without causing loops.

STP is a critical protocol for maintaining network stability and preventing network outages due to loops. However, it is important to note that STP has limitations, including potential delays in network convergence. Newer protocols like RSTP and MSTP address some of these limitations and provide faster convergence times, making them more suitable for modern Ethernet networks.

**Part – B**

**Steps:**

1. Establish a mesh network topology to interconnect network devices.

2. Disable the Spanning Tree Protocol (STP) on each switch by executing the command "No spanning-tree Vlan 1" via the terminal interface.

3. Upon executing the "Show spanning-tree" command, the display will indicate the absence of any spanning tree configurations.

4. Following the deactivation of the spanning-tree protocol, all network routes will transition to an enabled or 'green' state. Subsequently, initiate a broadcast from a device by pinging the IP address 192.168.10.255. This broadcast activity may lead to the generation of an unintended infinite loop.

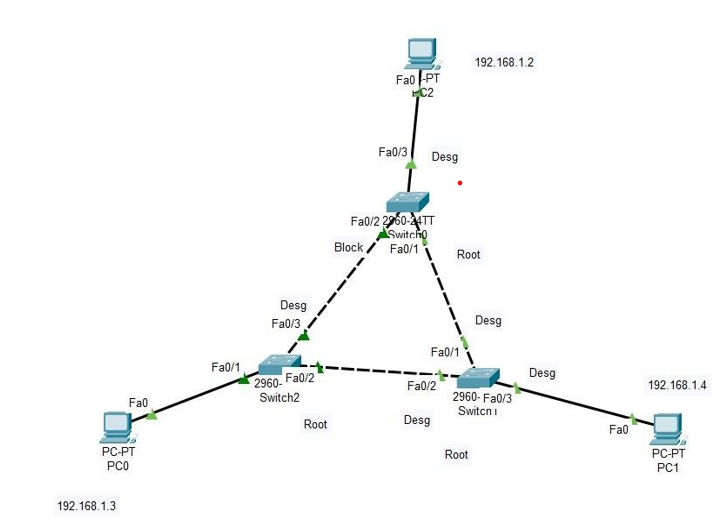
5. To mitigate the possibility of an infinite loop caused by the continuous exchange of broadcast packets, promptly re-enable the Spanning Tree Protocol by utilizing the command "Spanning-tree Vlan 1" within the terminal interface.

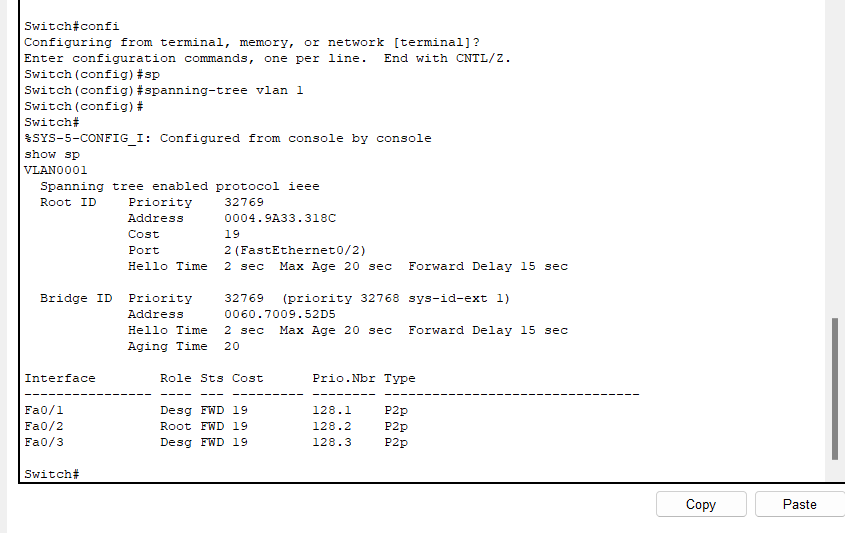
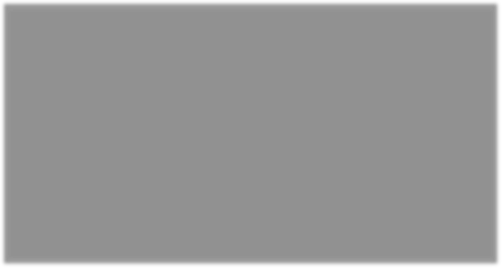
6. Broadcasting after reactivation will no longer induce an infinite loop in the network.

7. Then shutdown an enabled port (say, interface fast Ethernet 0/3) to enable a blocked port.

8. Subsequently, as the previously blocked port transitions to an enabled state, verify network connectivity by employing the "ping" command.

**Output:**





**Observation & Learning:**

While conducting a simulation of the Spanning Tree Protocol (STP) within the Cisco Packet Tracer environment, I had the opportunity to witness firsthand the protocol's inherent capability to thwart network loops by strategically selecting optimal routes to the root bridge while simultaneously blocking redundant links. The simulation underscored the intricacies of the root bridge election procedure, which hinges on Bridge IDs and priority settings, ultimately resulting in the establishment of a resilient network topology. Furthermore, this experiment effectively underscored STP's pivotal role in responding to dynamic topology alterations and ensuring network convergence, thereby emphasizing its critical importance in sustaining network reliability through the dual mechanisms of loop prevention and route optimization.

**Conclusion:**

To summarize, the simulation of the Spanning Tree Protocol (STP) within Cisco Packet Tracer served as a powerful illustration of its pivotal function in establishing a loop-free network topology. It achieved this by orchestrating the selection of a root bridge, optimizing path choices, and mitigating redundant link interference. This practical exercise underscored how STP plays a vital role in upholding network stability and mitigating performance disruptions arising from loop-related complications. As a result, it reinforced the significance of meticulous network planning and adept spanning tree management in the context of robust network infrastructure.

**Questions:**

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

**Ans:** Disabling Spanning Tree Protocol (STP) on all switches in a network can have significant consequences, primarily related to the risk of network loops and broadcast storms. Here is what can happen if STP is disabled:

**1) Network Loops:** Without STP to manage the network topology and block redundant paths, network loops can occur. A network loop is a situation where there are multiple paths between switches, and data packets can circulate endlessly within the loop. This can result in excessive network traffic and congestion, leading to network performance degradation or even a complete network outage.

**2) Broadcast Storms:** Network loops can cause broadcast storms, where broadcast packets multiply exponentially as they traverse the looped paths. Broadcast storms flood the network with unnecessary broadcast traffic, which can consume bandwidth, slow down network communication, and disrupt the normal operation of the network.

**3) Unpredictable Behaviour:** Disabling STP can lead to unpredictable behaviour in the network. The lack of loop prevention mechanisms means that network packets can take multiple paths, making it challenging to predict how data will flow through the network.

**4) MAC Address Table Instability:** Switches rely on MAC address tables to forward traffic efficiently. In a network without STP, the instability caused by looping can lead to MAC address table inconsistencies, making it challenging for switches to determine the correct forwarding path for frames.

**5) Downtime and Unavailability:** Network loops can cause network segments to become unreachable, leading to downtime for connected devices. This can impact critical services and applications relying on network connectivity.

**6) Network Instability:** Network stability is compromised when STP is disabled. Network administrators will have limited control over how traffic flows, and diagnosing and resolving network issues becomes more complex.

**7) Difficult Troubleshooting:** When network issues occur, troubleshooting becomes more challenging without STP. Identifying the root cause of network problems and locating loops can be time-consuming and frustrating.

In summary, disabling STP on all switches in a network is generally not recommended unless there are specific design requirements or constraints that necessitate doing so, and alternative loop prevention mechanisms are in place. If STP is disabled, it is essential to carefully manage the network topology, ensure redundant paths are controlled, and monitor the network closely to prevent or quickly mitigate any issues that may arise.

**2. What is mean by Designated, Root and Blk Interface?**

**Ans:** In the context of the Spanning Tree Protocol (STP), network interfaces on switches are categorized into three important states: Designated, Root, and Blocked (sometimes referred to as Forwarding, Root, and Disabled states, respectively). These states help STP create a loop-free topology in Ethernet networks.

**1) Designated Interface:**

- Designated interfaces are responsible for forwarding traffic on a specific network segment (usually a VLAN) within an Ethernet network.

- Each network segment elects a designated switch and, subsequently, a designated interface on that switch to be responsible for forwarding traffic onto the segment.

- The designated switch/interface is determined based on the lowest Bridge ID (BID). The switch with the lowest BID becomes the designated switch for that segment.

- Designated interfaces are in the Forwarding state, allowing them to pass traffic.

**2) Root Interface:**

- The root interface is the network interface on a switch that provides the fastest path to reach the Root Bridge, which is the central reference point in a spanning tree topology.

- All switches aim to have their best path (lowest-cost path) to the Root Bridge through their root interface.

- The root interface is in the Forwarding state and is typically the interface connected directly to the Root Bridge.

**3) Blocked Interface:**

- Blocked interfaces are those that have been intentionally placed in a blocking state by STP to prevent loops in the network.

- Blocked interfaces do not forward data frames but instead listen to the network to ensure loop prevention.

- The Blocking state is also known as the Disabled state in some versions of STP.

- The purpose of blocked interfaces is to eliminate redundant paths in the network, ensuring there are no loops.

Here are how these states work together:

- The Root Bridge is the reference point for all switches in the network. It has all its interfaces in the Forwarding state.

- Designated switches/interfaces are responsible for forwarding traffic toward the Root Bridge or within their designated network segments.

- Non-designated interfaces that are not part of the best path to the Root Bridge are placed in the Blocked (or disabled) state to prevent loops.

STP constantly monitors the network, and if there are changes (e.g., link failures or additions), it recalculates the spanning tree to ensure a loop-free topology. This process can involve transitioning interfaces between the Designated, Root, and Blocked states as needed to adapt to network changes and maintain network stability.

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

**Ans:** In the Spanning Tree Protocol (STP), identifying the root bridge is a crucial step in determining the network's spanning tree topology. The root bridge serves as the reference point for all switches in the network. There are several ways to identify the root bridge in STP:

**1) Lowest Bridge ID (BID):**

- Each switch in an STP network is assigned a unique Bridge ID (BID), which is a combination of a priority value and the switch's MAC address.

- The switch with the lowest BID becomes the root bridge.

- The BID is used to determine the root bridge during the initial election process.

**2) Priority Value:**

- The Bridge ID priority value is a configurable parameter (ranging from 0 to 65535) that can be set on each switch.

- By default, all switches have a priority of 32768.

- Lower priority values indicate a higher likelihood of becoming the root bridge. You can manually set the priority value on a switch to influence the root bridge election.

**3) MAC Address:**

- If two or more switches have the same priority value in their BIDs, the MAC address is used as a tiebreaker.

- The switch with the lowest MAC address becomes the root bridge.

**4) Bridge Identifier (BID):**

- The BID is a combination of the priority value and the MAC address. It is typically represented as a 16-bit priority field followed by a 48-bit MAC address.

- BIDs are compared during the root bridge election process to determine the root bridge.

**5) Bridge Protocol Data Unit (BPDU):**

- BPDU frames are used by switches to communicate with each other and exchange information about the network topology, including the BID of the sending switch.

- Through the exchange of BPDUs, switches gather information about the BIDs of other switches in the network and use this information to elect the root bridge.

**6) Election Process:**

- The root bridge election process begins with all switches in the network considering themselves as the root bridge.

- They send out BPDUs containing their BID and receive BPDUs from other switches.

- By comparing the BID are received BPDUs, switches gradually determine which switch has the lowest BID, making it the root bridge.

- The root bridge periodically sends BPDUs to announce its status, and other switches forward these BPDUs through the network to maintain awareness of the root bridge.

In summary, the root bridge in STP is identified through a combination of factors, including Bridge ID priority values, MAC addresses, and the exchange of BPDUs. The switch with the lowest BID becomes the root bridge, and its role is to define the spanning tree topology for the entire network, ensuring a loop-free path for data traffic.