Usman Institute of Technology

Department of Computer Science

Course Code: CS222

Course Title: Data Communication & Computer Networks

Fall 2022

Lab 08

Objective:

Avoiding Broadcast storms using spanning tree protocol and Implementing port security

Student Information

Student Name	
Student ID	
Date	

Assessment

Marks Obtained	
Remarks	
Signature	

Usman Institute of Technology
Department of Computer Science
CS222- Data Communication & Computer Networks

Lab 03

Instructions

State the instruction that student needs to follow for performing the example and exercises. Some sample instructions are given below which can be altered as needed
E.g.

- Come to the lab in time. Students who are late more than 15 minutes, will not be allowed to attend the lab.
- Students have to perform the examples and exercises by themselves.
- Raise your hand if you face any difficulty in understanding and solving the examples or exercises.
- Lab work must be submitted on or before the submission date.

1. Objective

Avoiding Broadcast storms using spanning tree protocol and Implementing port security

2. Labs Descriptions

2.1 Spanning Tree protocol (STP)

It's a layer two protocol that makes a topology loop free and it runs on bridge and switch. redundant paths are formed to ensure backup routes in case if there is a disaster or lapse in one of the links, with redundant links there is a problem that packet circulates in the same cycle, when we use spanning tree it helps break those loops by disabling a port that is responsible for creating a loop. The IEEE standard for spanning tree is 802.1D.

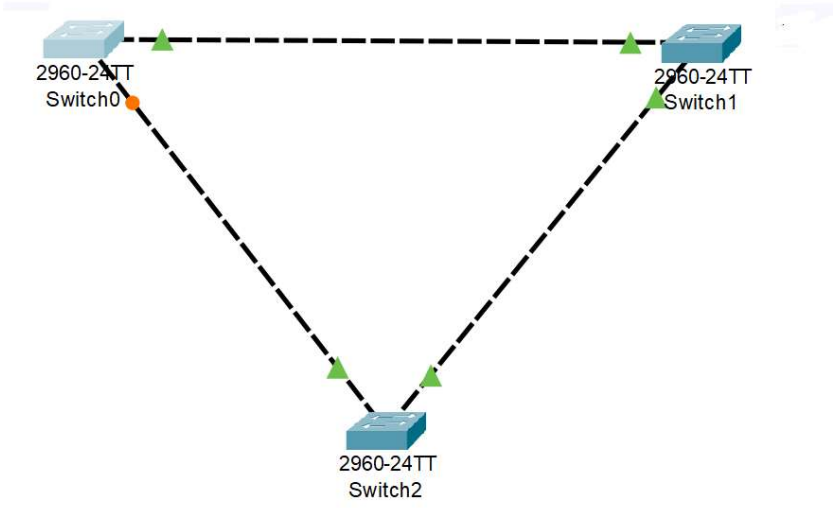

Figure 1: Depicting the spanning tree enabled network

The above scenario depicts that under such circumstances where there is a loop and if spanning tree is not activated then problem of broadcast storms rises. Fortunately above image has spanning tree protocol activated.

Spanning-tree vlan 1

As one can see one of the link causing loop was deactivated by spanning tree protocol hence preventing broadcast storms.

2.2 Election of the Spanning-Tree Root

Initially the concept was implemented with the bridges and later on switches also used spanning tree protocol therefore while using STP the term used is called selection of root bridge, All bridges in the Layer 2 network that are participating in STP gather information about other bridges in the network by exchanging BPDU data messages. This message exchange results in these actions:

i. The election of a unique spanning-tree root for each spanning-tree instance

ii. The election of a designated bridge for every LAN segment

iii. The removal of loops in the network by blocking Layer 2 interfaces connected to redundant links

For each VLAN, the bridge with the highest bridge priority (the lowest numerical priority value) is elected as the spanning-tree root. If all bridges are configured with the default priority (32768), the bridge with the lowest MAC address in the VLAN becomes the spanning-tree root. The bridge priority value occupies the most significant bits of the bridge ID.

When you change the bridge priority value, you change the probability that the bridge will be elected as the root device. Configuring a higher value decreases the probability; a lower value increases the probability.

The spanning-tree root is the logical center of the spanning-tree topology. Paths that are not needed to reach the spanning-tree root from anywhere in the network are placed in the spanning-tree blocking mode.

BPDUs contain information about the sending bridge and its ports, including bridge and MAC addresses, bridge priority, port priority, and path cost. STP uses this information to elect the spanning-tree root and root port for the network and the root port and designated port for each LAN segment.

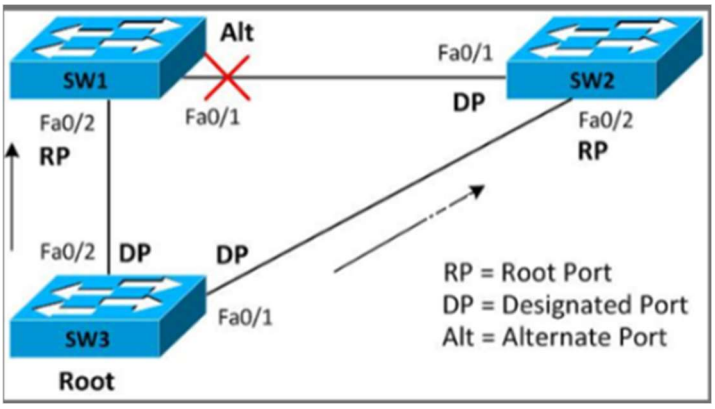

Figure 2: Depicting the Root Bridge selection and assignment of root port, designated port and alternate port

2.3 Spanning-Tree Interface States

Propagation delays can occur when protocol information passes through a wireless LAN. As a result, topology changes can take place at different times and at different places in the network. When an interface transitions directly from nonparticipation in the spanning-tree topology to the forwarding state, it can create temporary data loops. Interfaces must wait for new topology information to propagate through the LAN before starting to forward frames. They must allow the frame lifetime to expire for forwarded frames that have used the old topology.

Each interface on a bridge using spanning tree exists in one of these states:

- Blocking—The interface does not participate in frame forwarding.
- Listening—The first transitional state after the blocking state, in which the spanning tree determines that the interface should participate in frame forwarding.
- Learning—The interface prepares to participate in frame forwarding.
- Forwarding—The interface forwards frames.
- Disabled—The interface is not participating in spanning tree because there is a port shutdown, there is no link on the port, or no spanning-tree instance is running on the port.

An interface moves through these states:

- From initialization to blocking
- From blocking to listening or to disabled

- From listening to learning or to disabled
- From learning to forwarding or to disabled
- From forwarding to disabled

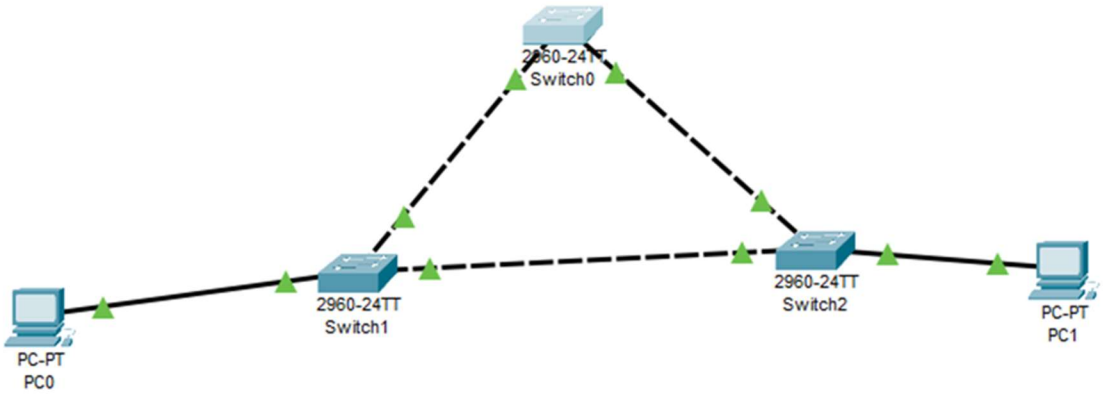

Figure3 : Depicting a network topology without spanning tree protocol

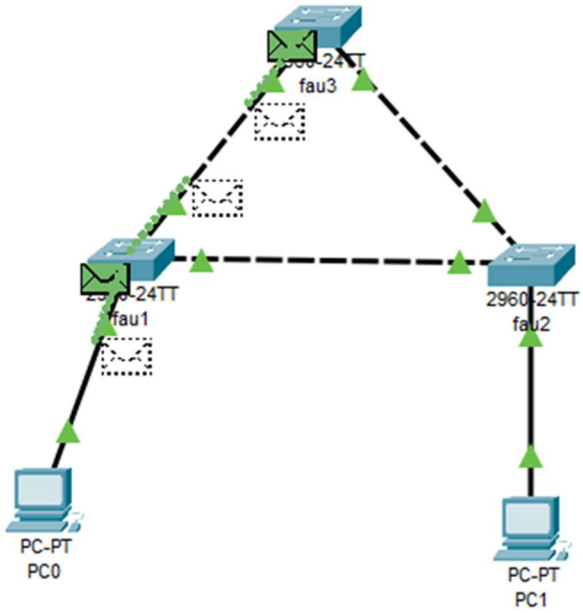

Figure4 : Broadcast Storms because of absence of spanning tree

2.4 Port Security

Each port of a switch has the capacity to learn 132 mac addresses, if we want to implement security so no unauthorize user can connect their device with the network we can implement the concept of port security. This implementaion is done at the configuration mode of the switch, after applying port security

we can limit the number of users that can get connected with that port of the switch and in case of violation we can also specify the response.

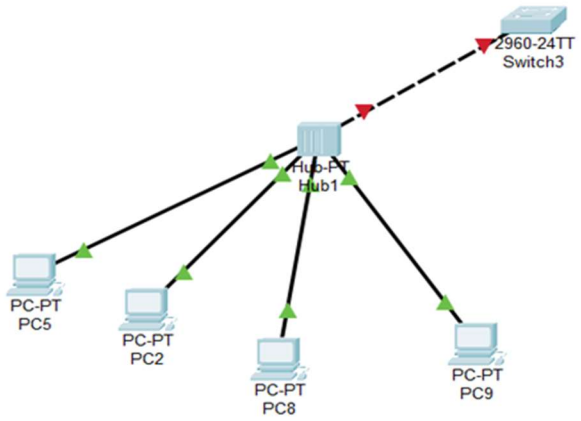

Figure 5: Port security implemented to limit the attached systems to three when fourth node is connected the link goes down

The above diagram shows that after connecting the fourth PC the link between hub and switch went in to the shutdown state it means that security was implemented which stated that if more than three devices connects to one port of the switch then the link connecting switch and hub should go down.

Switchport port-security

Lab Task

1) Implement spanning tree in a topology mentioned in figure 1, study the behavior of network in presence and absence of spanning tree protocol, take screen shots and describe the how network will behave [Observe in Simulation mode]

2) Implement the topology mentioned in figure 5, configure it in such away that it can accommodate only 4 nodes and gets shutdown when 5th is attached