Title:

Study on L2 Switches.

Problem Statement:

1. Formation of MAC Address Table and updating MAC address table.
2. ARP Table formation and Study of Spanning Tree Protocol.
3. Switch vs Hub
4. VLANs

Resources:

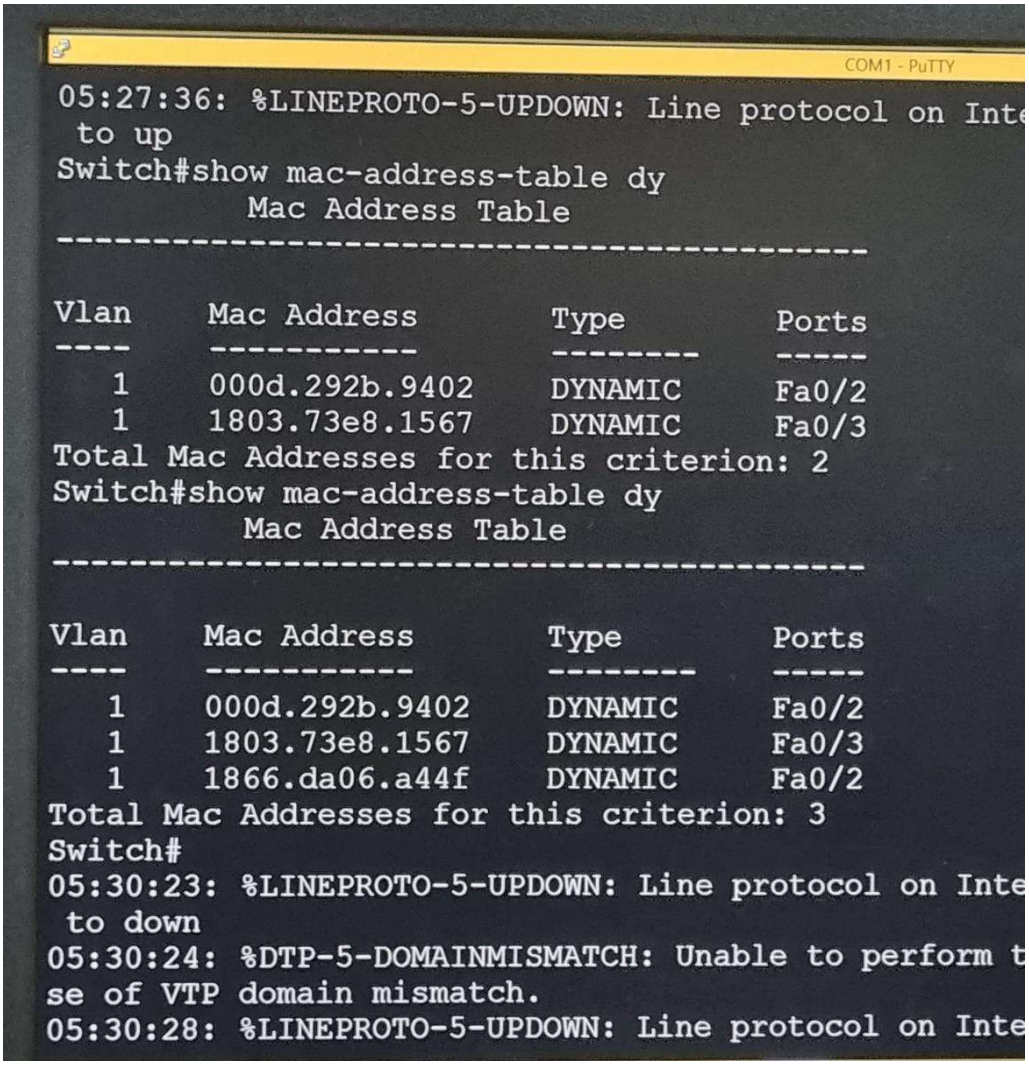
L2 switches, Hub, PC's, and RJ45 Connector.

Brief Theory & Background:

- **[1.]MAC ADDRESS**: A MAC (Media Access Control) address is a unique identifier assigned to a network interface controller (NIC) for communications at the data link layer of a network segment. It's also known as a hardware address or physical address. MAC addresses are typically assigned by the manufacturer of the network interface and are stored in the device's hardware. MAC addresses are usually represented as a series of six pairs of hexadecimal digits, separated by colons or hyphens. For example, a MAC address might look like this: 00:1A:2B:3C:4D:5E.

- **Formation and Update a MAC address table**: Consider a scenario within a Local Area Network (LAN) where devices are interconnected via a switch. When a device within this network seeks to engage in communication with another device, it transmits an Ethernet frame containing its MAC address. This MAC address is then scrutinized by the switch, which proceeds to map the MAC address to the port through which the Ethernet frame was received. This mapping process is dynamic, constantly monitoring ports and their associated MAC addresses. Whenever a destination MAC address is not found within the table, the switch updates its MAC address table accordingly. Moreover, to ensure the efficiency of network resources, entries within the MAC address table are subject to removal if there's been no communication activity associated with a specific MAC address for an extended duration. This continuous process enables the formation and maintenance of an up-to-date MAC address table, facilitating efficient data transmission within the LAN.

- **Output:**

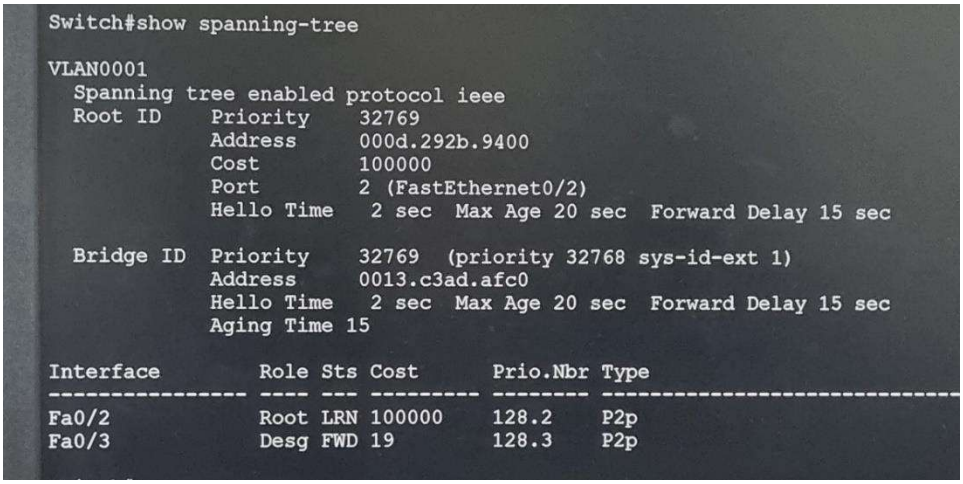


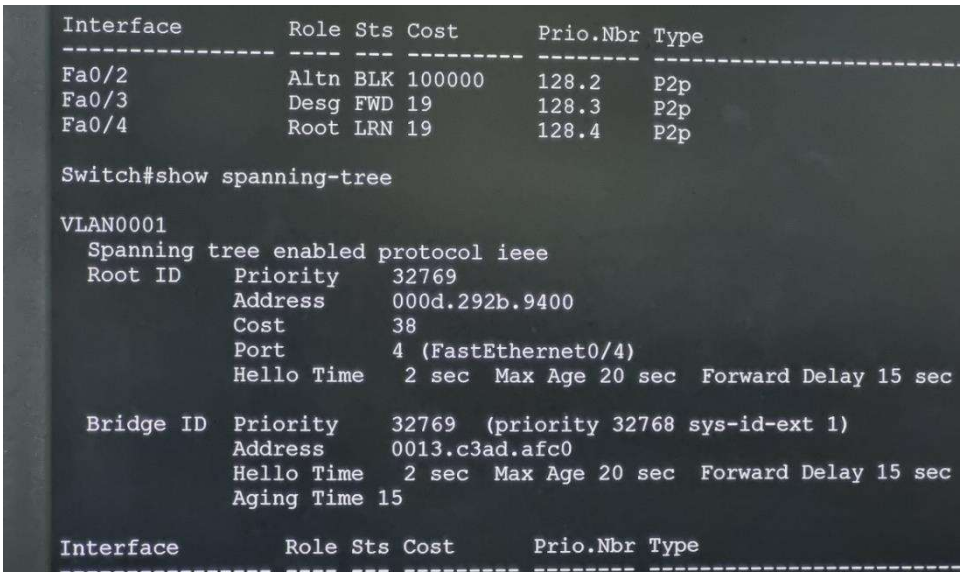
- **Discussion:** First/initially I tried to established a connection from port of each switch to every device on that same network have. Then I noticed that output which came on screen, where we can see the MAC address of every PC's/device that connected with which port. Then after alternating the port connection with different different devices, I observed that MAC address is updated or not.

- **[2.]ARP Table Formation and study of spanning tree protocol:**
  ARP, or Address Resolution Protocol, is crucial in networking. It helps devices on a network locate each other by finding their MAC addresses. This actually doing the seamless data transmission within a Local Area Network (LAN).

  The Spanning Tree Protocol (STP) ensures network efficiency by designating a root node and calculating the shortest paths to it for switches. This resists loops and congestion. STP adapts to network changes, adjusting traffic flow. Path costs, determined by bandwidth, dictate the optimal routes within the spanning tree.

- **OUTPUT**:





- **Discussion:** Initially, when devices are not connected with each other's addresses, data transmission occurs haphazardly, with packets sent out indiscriminately. Upon receiving data, the destination device responds with its MAC address, facilitating the switch's construction of an ARP table with all corresponding IP & MAC addresses. For SPT part as I noticed that a root bridge is designed in such a way that which device has lowest designate that. Then it map's out the most efficient route to other node/device. So it's means adapting dynamically to change the network topology.

- **[3.] Switches Vs Hubs:** Switches and hubs are both networking devices used to connect multiple devices within a local area network (LAN).

  A switch operates at the data link layer (Layer 2) of the OSI model. It forwards data packets based on the MAC addresses of the devices connected to it. Switches have multiple ports, and each port operates independently. It offers full-duplex communication. Switches are more intelligent than hubs because they maintain a MAC address table, which helps in efficient packet forwarding. Switches are generally faster and more efficient than hubs because they reduce network congestion by sending data only to the intended recipient.

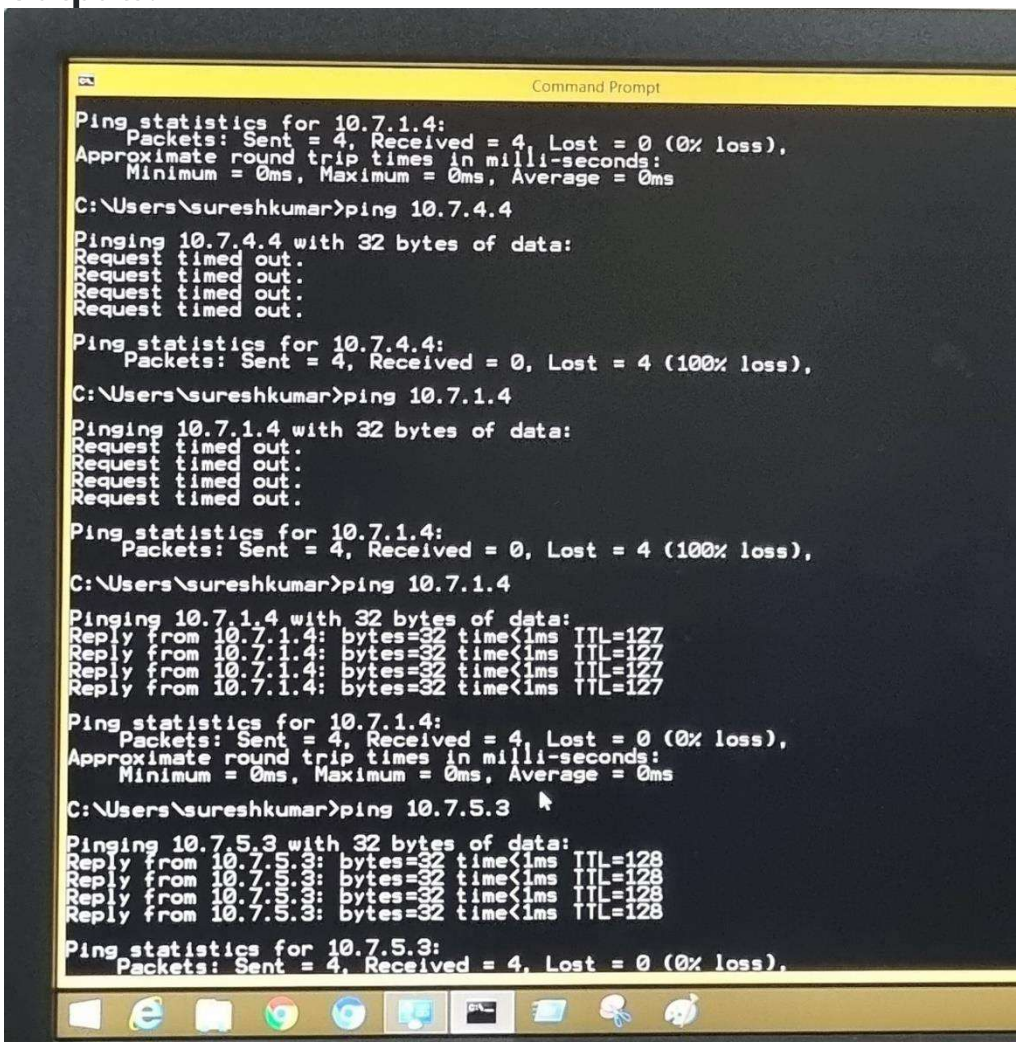
  A hub operates at the physical layer (Layer 1) of the OSI model. It receives data packets from one device and broadcasts them to all other devices connected to the hub. Hubs do not have any intelligence to determine where to send data packets. Hubs operate in half-duplex mode, meaning data can be transmitted or received, but not both simultaneously.

  switches are the preferred choice for connecting devices in a LAN due to them intelligence, efficiency, and ability to reduce network congestion. Data rates are shown in the below figure:

- **Outputs:** iteration value after 3/4 times speed, I got
  10954kbps
  11311kbps
  11878kbps
  11130.05kbps.
- **Discussions:** Consider the LAN network with some switches have many ports in that same network. After that connection with that switches with ports and then send a file from one switch to another, then I noticed the data speed from each switch and by changing bandwidth, also noticed that how much speed I got when many switches are communicated at same time means the data rate decreases. but in case of hubs send the data between switch and Hub, data speed was less compared to switches remaining same process. If more switches connected to Hub, then I observed that send the data at a time two switches, data speed is more compared to switches operation based on bandwidth. Because switch could send the data based on MAC address to respective destination node

but in hub send data to all nodes whether it is destined for a particular destination or not. So Hubs send with high speed compared to switch network.

- **[4.] Functions of VLAN'S:** A VLAN (Virtual Local Area Network) is a method of dividing a network into separate logical segments, achieved primarily through the use of Layer 2 and Layer 3 switches. By implementing VLANs, devices or computers can be organized into distinct networks within a single physical infrastructure, allowing for efficient management. VLAN configurations are typically established using routers to segregate different physical networks and then subdividing them into smaller subnetworks. setup done by using a router to separate two physical networks and then creates into subnetwork which does not communicate any other network directly.
- **Outputs:**



- **Discussions:** At first, I learned about MAC address of each L2 switches. Each switch is connected to another switches with router connected network. Also, each switch transfer the data with different rate and also have a specific Bandwidth. But function VLAN sperate the network into subnetwork, break the

connection by L3 switch. All switches connected to L3 switch then connection between subnetwork breaks (trunk encapsulation), ports of each switch connected via L3 switch. This observation shows the functionality of L3 switches in preventing direct data exchange between switches within the same network. Consequently, it can be inferred that VLANs effectively segment the network into subnetworks, thereby restricting communication between them.

- **Conclusions:**
  The study of working of different functions of L2 switch and L3 switch is done on random LAN network and also learned about the MAC table formation and ARP and SPT formation.