Name: Shubhan Singh

Class: SE Comps B

Roll no.:2022300118

CCN Experiment 3

Aim: Network Devices, Topology and Design

Part 1: Network Devices

A network device is a piece of hardware or software integral to communication between a computer and an internet network. Network devices play two roles. The first is establishing a network connection, as a router or a modem does. The second one is maintaining, protecting and enhancing that connection, as with a hub, repeater, switch or gateway.

Following are notes on some of the networking devices:

1. **Bridge**

   Bridges connect two or more hosts or network segments by storing or hosting frames between them. Bridges use hardware MAC addresses for transferring frames. They can forward or block data with the MAC address of the devices connected to each segment. They can also connect two physical LANs into a larger logical LAN. Bridges work in the data link layer of the OSI model. Bridges can be set up using two models:
   - Local bridging establishes LAN connections with local cables.
   - Remote bridging brings two connections together via a wide area network (WAN).
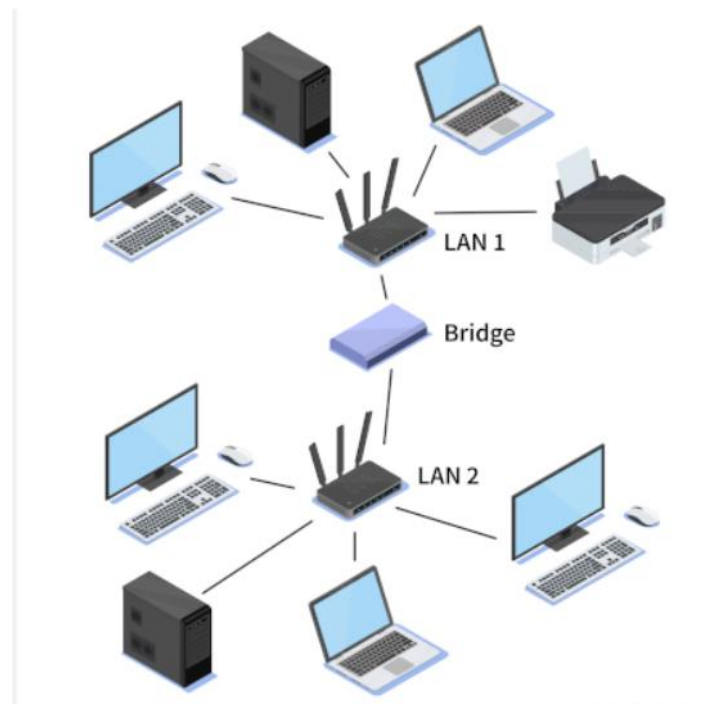
Bridges are like hubs in many respects, including connecting LAN components with identical protocols. However, bridges filter incoming data packets, known as frames, for addresses before being forwarded. As it filters frames, the bridge makes no modifications to the formatting or content of the incoming data. Instead, the bridge filters and forwards frames on the network with the help of a dynamic bridge table. The bridge table, which is initially empty, maintains the LAN addresses for each computer in the LAN and the addresses of each bridge interface that connects the LAN to other LANs. Bridges, like hubs, are either simple or multiple-port.

2. Hub

Hubs connect multiple computer networking devices, working only on the Physical layer of the OSI. Hubs do not perform packet filtering or addressing functions as they have no routing tables or intelligence (unlike a network switch or router). Instead, they send data packets to all connected devices. A hub also acts as a repeater, amplifying signals that deteriorate after traveling long distances over connecting cables. A hub is the most straightforward network connecting device because it connects LAN components with identical protocols.
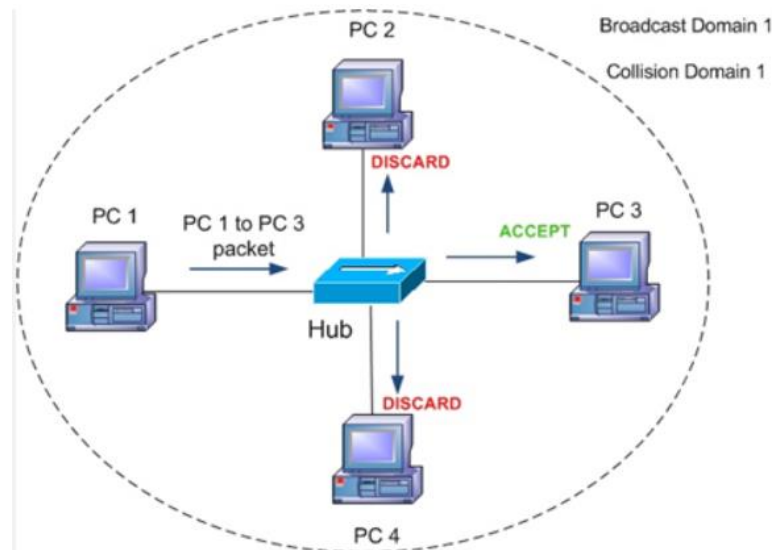
A hub can be used with digital and analog data, provided its settings are configured to prepare for the formatting of the incoming data. For example, if the incoming data is in digital format, the hub must pass it on as packets. But if the incoming data is analog, it passes it on in signal form.

There are 3 main types of hubs:

- **Passive Hub**: These are the hubs that collect wiring from nodes and power supply from the active hub. These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend the distance between nodes.
- **Active Hub**: These are the hubs that have their power supply and can clean, boost, and relay the signal along with the network. It serves both as a repeater as well as a wiring center. These are used to extend the maximum distance between nodes.
- **Intelligent Hub**: It works like an active hub and includes remote management capabilities. They also provide flexible data rates to network devices. It also enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.

3. **L-2 Switch**

A layer 2 switch is a type of network switch or device that works on the data link layer (OSI Layer 2) and utilizes MAC Address to determine the path through where the frames are to be forwarded. It uses hardware based switching techniques to connect and transmit data in a local area network (LAN). A layer 2 switch can also be referred to as a multiport bridge.

A layer 2 switch is primarily responsible for transporting data on a physical layer and in performing error checking on each transmitted and received

frame. A layer 2 switch requires MAC address of NIC on each network node to transmit data. They learn MAC addresses automatically by copying MAC address of each frame received, or listening to devices on the network and maintaining their MAC address in a forwarding table. This also enables a layer 2 switch to send frames quickly to destination nodes. However, like other layer switches (3,4 onwards), a layer 2 switch cannot transmit packet on IP addresses and don't have any mechanism to prioritize packets based on sending/receiving application.

4. **L-3 Switch**

Also called a multilayer switch, it is a specialized hardware device that has a lot in common with the traditional router—both in physical appearance and function. Layer 3 switches support the same routing protocols as routers and inspect incoming packets, as well as make vital routing decisions the same way routers do. And they do these routing tasks in addition to performing switching duties. Like routers, Layer 3 switches can be configured to support such routing protocols as:

- Routing Information Protocol (RIP)
- Open Shortest Path First (OSPF)
- Enhanced Interior Gateway Routing Protocol (EIGRP)

These switches were designed to improve the network routing performance on large local area networks (LANs) such as intranets.

While Layer 2 switches can route data traffic dynamically when there is low to medium traffic, their performance suffers when it increases to a high level.

The main difference between a router and a Layer 3 switch lies inside the hardware itself. Layer 3 switch hardware combines that of traditional switch and routers—replacing some of the typical router software with integrated circuit hardware that provides better LAN performance. In addition, a Layer 3 switch will not usually have wide area network (WAN) ports which are standard in routers.

5. Router

The router is a physical or virtual internetworking device that is designed to receive, analyze, and forward data packets between computer networks. A router examines a destination IP address of a given data packet, and it uses the headers and forwarding tables to decide the best way to transfer the packets. Some important points about routers are given below:

- A router is used in LAN (Local Area Network) and WAN (Wide Area Network) environments.
- It shares information with other routers in networking.
- It uses the routing protocol to transfer the data across a network.
- Furthermore, it is more expensive than other networking devices like switches and hubs.

A router works on the third layer of the OSI model, and it is based on the IP address of a computer. It uses protocols such as ICMP to communicate between two or more networks. *It is also known as an* intelligent device *as it* can calculate the best route to pass the network packets from source to the destination automatically.
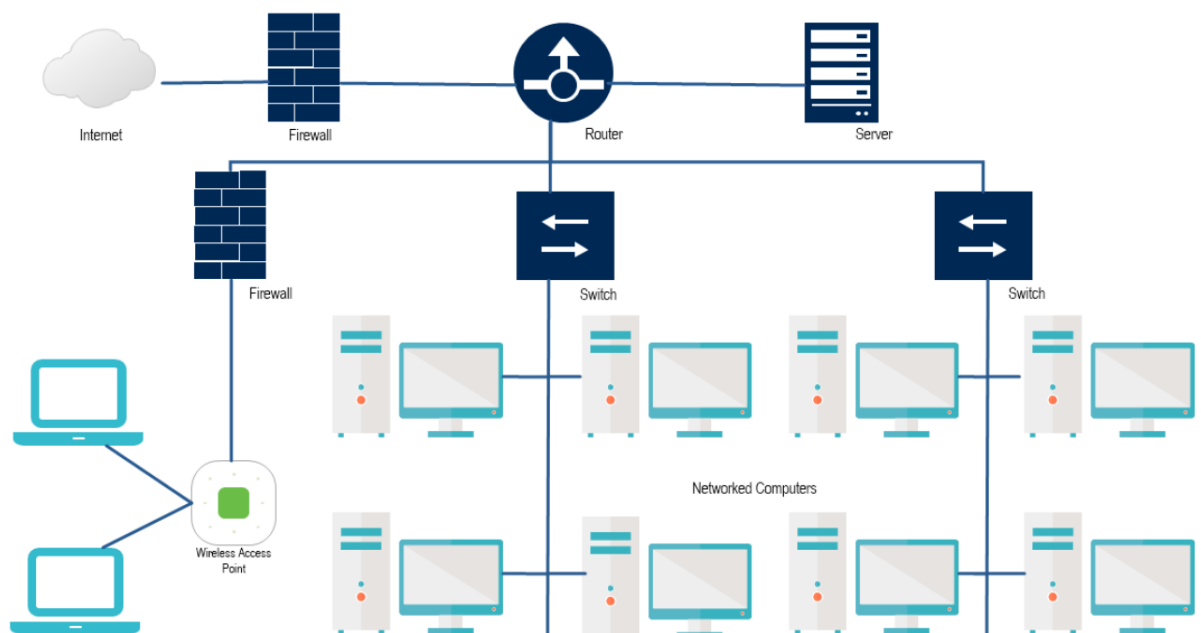
6. WiFi router

A wireless router, also called a Wi-Fi router, combines the networking functions of a wireless access point and a router. It is a fundamental networking device that facilitates the connection of devices within a local area network (LAN) to the broader internet. Operating as a router, it directs data packets between different networks based on IP addresses, while Network Address Translation (NAT) allows multiple devices to share a single public IP

address. Offering both wireless (Wi-Fi) and wired (Ethernet) connectivity, routers serve as a gateway for devices such as smartphones, laptops, and smart home gadgets.

They often include built-in firewalls, DHCP servers for automatic IP address assignment, and features like Quality of Service (QoS) settings, firmware updates, and guest network support, enhancing security, performance, and flexibility in managing network traffic.

Part-2: Network topologies

In Computer Network ,there are various ways through which different components are connected to one another. Network Topology is the way that defines the structure, and how these components are connected to each other.

Some of the commonly used network topologies are as follows:

1. **Bus topology**

   Alternatively mentioned as line topology, bus topology is a topology in which which each computer and network device is connected to a minimum of one Common cable or backbone.
   Bus topology carries transmitted data through the cable. because data reaches each node, the node checks the destination address (MAC/IP address) to work out if it matches their address. Data is transferred if the address in the message matches that of the node. In the bus, communication between nodes is done through a foremost network cable.
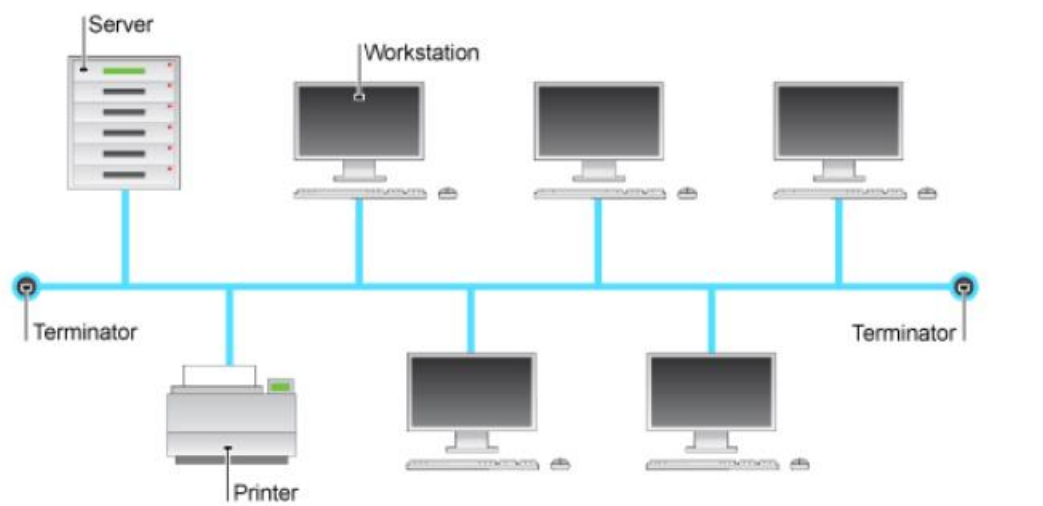
   Advantages of Bus Topology :
   - It is the easiest network topology for connecting peripherals or computers in a linear fashion.
   - It works very efficiently well when there is a small network.

- It is easy to connect or remove devices in this network without affecting any other device.
- Very cost-effective as compared to other network topology i.e. mesh and star

Disadvantages of Bus Topology :
- Bus topology is not great for large networks.
- Identification of problems becomes difficult if the whole network goes down.
- Troubleshooting individual device issues is very hard.
- Need terminators are required at both ends of the main cable.
- Additional devices slow the network down.
- If the main cable is damaged, the whole network fails or splits into two.
- Packet loss is high.

2. **Ring topology**

Ring topology may be a network configuration where device connections create a circular data path. In this each device is connected to with its exactly two neighbouring devices, like points on a circle which forms like a ring structure. A number of repeaters are used for Ring topology with a large number of nodes to send data and to prevent data loss repeaters are used in this network. Together, devices during a ring topology are mentioned as a hoop network. In this packets travels from one device to another until they reach the desired destination. Here data travels in unidirectionally but it can also do bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology. It is used in LANs and WANs depending on the card of network in the computer.
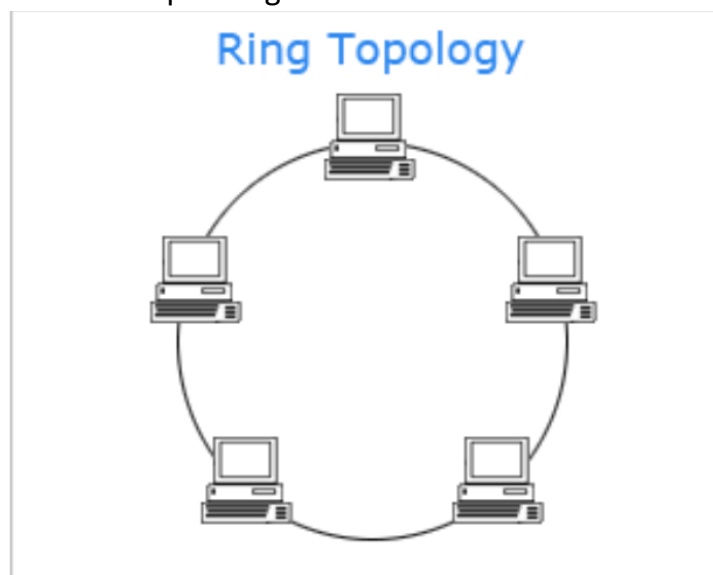
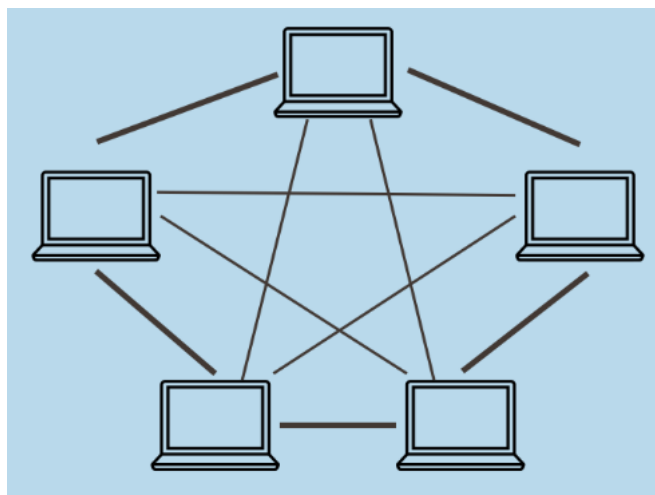Ring Topology

Advantages of Ring topology :

- In this data flows in one direction which reduces the chance of packet collisions.
- In this topology additional workstations can be added after without impacting performance of the network.
- Equal access to the resources.
- It is cheap to install and expand.
- Minimum collision.
- Speed to transfer the data is very high in this type of topology.
- Due to the presence of token passing the performance of ring topology becomes better than bus topology under heavy traffic.

Disadvantages of Ring topology :

- Due to the Uni-directional Ring, a data packet (token) must have to pass through all the nodes.
- If one workstation shuts down, it affects whole network or if a node goes down entire network goes down.
- In order for all the computer to communicate with each other, all computers must be turned on.

3. Mesh

In mesh, all the computers are interconnected to every other during a network. Each computer not only sends its own signals but also relays data from other computers. The nodes are connected to every other completely via a dedicated link during which information is travel from nodes to nodes and there are N(N-1)/2 links in mesh if there are N nodes. Every node features a point-to-point connection to the opposite node. The connections within the mesh can be wired or wireless.

There are two types of Mesh topologies –
1. Fully-connected Mesh Topology
2. Partially-connected Mesh Topology

1. Full Mesh Topology :

All the nodes within the network are connected with every other If there are n number of nodes during a network, each node will have an n-1 number of connections. A full mesh provides an excellent deal of redundancy, but because it is prohibitively expensive to implement, it's usually reserved for network backbones.
Total number of links required for the mesh topology is [n(n-1)]/2.

2. Partial Mesh Topology :

In a partially connected mesh, all the nodes aren't necessary to be connected with one another in the network. Peripheral networks are connected using partial mesh and work with a full-mesh backbone in tandem.

Advantages of Mesh Topology :
- Failure during a single device won't break the network.
- There is no traffic problem as there is a dedicated point to point links for every computer.
- Fault identification is straightforward.
- It provides high privacy and security.
- Adding new devices won't disrupt data transmissions.

Disadvantages of Mesh Topology :
- It's costly as compared to the opposite network topologies i.e. star, bus, point to point topology.
- Installation is extremely difficult in the mesh.
- There is a high risk of redundant connections.
- Each node requires a further utility cost.
- Maintenance needs are challenging with a mesh.

4. Star topology

A star may be a topology for a Local Area Network (LAN) during which all nodes are individually connected to a central connection point, sort of a hub or a switch. A star takes more cable than e.g. a bus, but the benefit is that if a cable fails, just one node is going to be brought down. Each device within the network is connected to a central device called a hub. If one device wants to send data to another device, it's to first send the info to the hub then the hub transmits that data to the designated device. The number of links required to connect nodes in the star topology is N where N is the number of nodes.
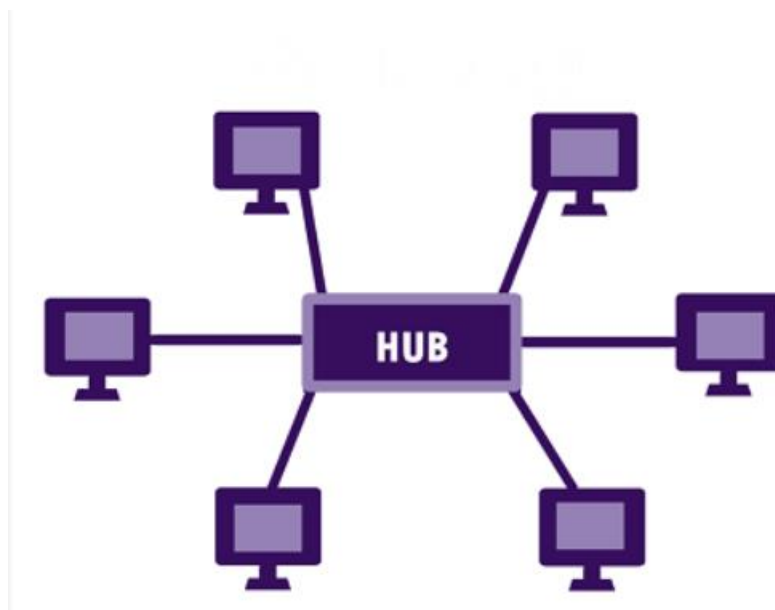
Unlike Mesh topology, a device cannot provide communication directly between the devices in a star topology, it has to communicate with the help of a hub. The peripheral devices function as clients, while the central network device serves as a server. Depending on the kind of network card installed in each computer, the RJ-45 or coaxial cable is used in a star topology. Like a Bus Topology, establishing a computer network that employs star topology is very straightforward and easy.

Advantages of Star Topology

- It is very reliable – if one cable or device fails then all the others will still work

- It is high-performing as no data collisions can occur

- Less expensive because each device only need one I/O port and wishes to be connected with hub with one link.

- Easy fault detection because the link are often easily identified.

- No disruptions to the network when connecting or removing devices.

Disadvantages of Star Topology

- If the connecting network device (network switch) fails, nodes attached are disabled and can't participate in network communication.

- More expensive than linear bus topology due to the value of the connecting devices (network switches)

- Performance is predicated on the one concentrator i.e. hub.

5. Hybrid topology

Topology may be a connection of varied links and nodes, communicating with one another for the transfer of knowledge. During this process sort of topology, we combine two or more different topologies to make a resultant topology that has good points(as well as weaknesses) of all constituent basic topologies instead of having characteristics of only one specific topology. This mix of topologies is completed and consistent with the wants of the organization.

Example for instance if in an office one of the department's ring topologies is employed and another star, topology is employed, connecting these topologies will end in Hybrid Topology.

Some of the common hybrid topologies are:-

- Star-Ring Hybrid Topology

- Star-Bus Hybrid Topology

- Hierarchical network topology
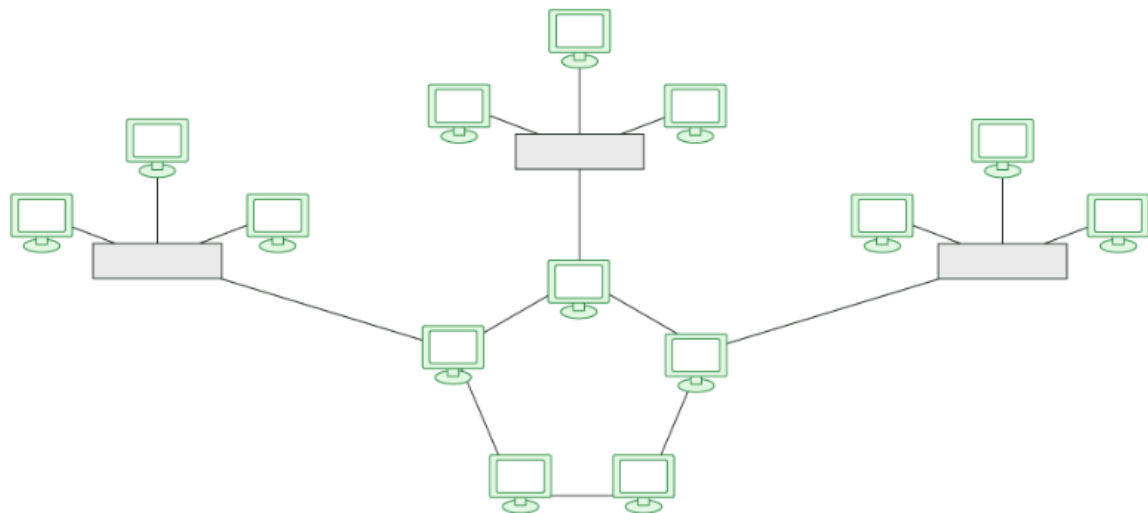
Star-Ring Hybrid Topology

Advantages of Hybrid Topology

- This type of topology combines the benefits of different types of topologies in one topology.

- Can be modified as per requirement.

- It is easily scalable as Hybrid networks are built in a fashion which enables easy integration of new hardware components.

- Error detecting and troubleshooting are easy.

- Handles a large volume of traffic.

- It is used to create large networks.

Disadvantages of Hybrid Topology

- It is expensive.

- The design of a hybrid network is very complex.

- There is a change in the hardware to connect one topology with another topology.

- Usually, hybrid architectures are larger in scale so they require a lot of cables in the installation process.

Part-3: Network Design

Shubhan Singh
2022300118
SE comps B

Exp 3 - network design.

Campus network design
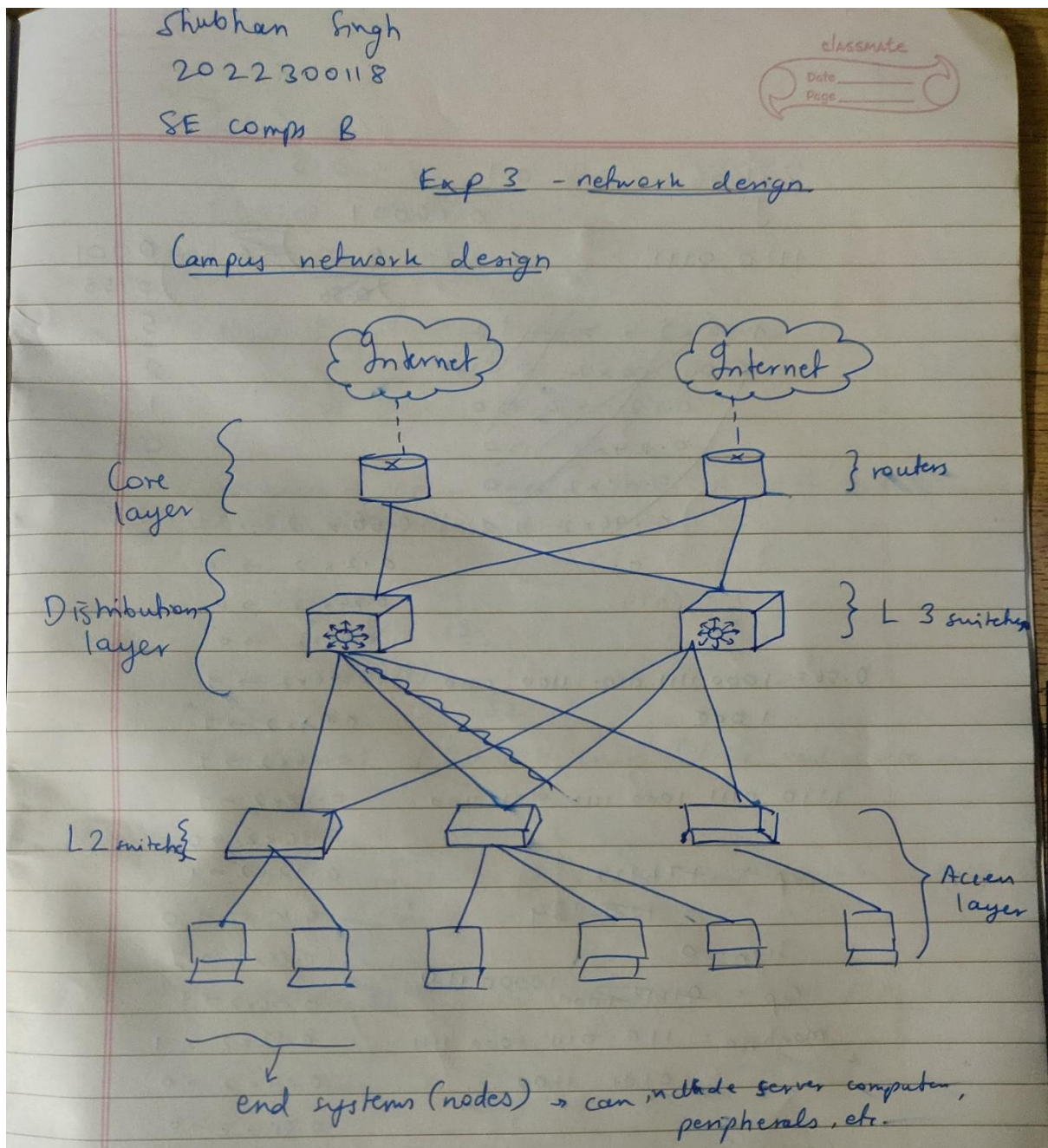
This network design is based on the 3 Tier architecture.

The three layers are:

1. **Access layer:** Access Layer is the lowest layer of 3 Tier Architecture. It is the closest layer to the end users. In this Access Layer, L-2 Switches resides and end systems are connected to these switches.

2. **Distribution layer:** Distribution Layer is the middle layer of 3 Tier Architecture. This layer works as the bridge between Access Layer and Core Layer. Instead of Access layer switches, multilayer (L-3) switches are used in Distribution layer.
   Redundancy is used in this layer to overcome single point of failure. Multiple Multilayer switches are used as redundant in this layer. Distribution policies are also used in this layer.

3. **Core layer:** Core layer is also known as Backbone Network. Core (Backbone) Layer connects distribution layer devices. It is made of of high speed packet switching routers.
   Routing protocols are used in this layer and the main duty of this layer is providing routing between them and the distribution layer.
   Redundancy is also important feature of this layer. So, redundant core devices are used to overcome single point of failure.
   The core layer is connected then to the internet, it is designed to be always on.

- This design has lots of redundancy to guard against failures at singular points and guards against interruptions in service. It is expensive to implement though, and is intended for larger networks, like college campuses.