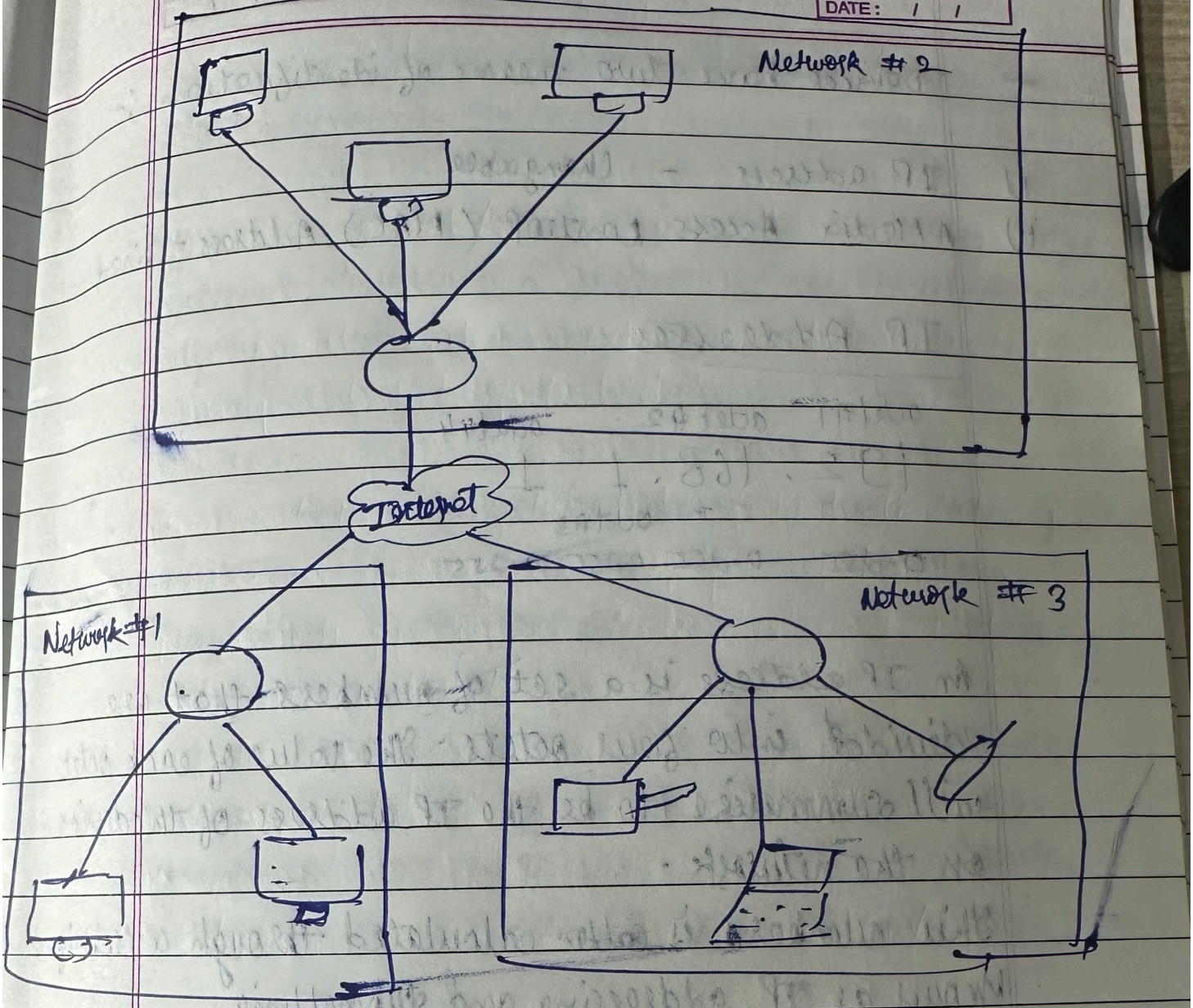
Computer Networking

PAGE NO.
DATE : / /



The internet is made up of many small networks all joined together. These small networks are called private networks, where networks connecting these small networks are called public networks — of the internet.

So, there can be two types of networks :-

i) Public network
ii) Private network

- Devices have two means of identification ;-

i) IP address - Changable
ii) A Media Access Control (MAC) Address - fixed

IP Addresses

octet#1 octet#2 octet#3 octet#4

192.168.1.1

0-255 0-255 0-255 0-255

An IP address is a set of numbers that are divided into four octets. The value of each octet will summerise to be the IP address of the device on the network.
This numbers is ~~eeee~~ calculated through a technique knows as IP addressing and subnetting.
IP addresses can change from device to device but cannot be active simultaneously more than once within the same network.

IP addresses follow a set of standards known as protocols. These protocols are backbone of networking and force many devices to communicate in the same language.

Devices can be on both a private and public network depending on where they are will determine what

PAGE NO.
DATE : / /

type of IP address they have : public or private IP address.

A public address is used to identify the device on the internet, whereas a private address is used to identify a device amongst other devices.

Example :-

Here we have two devices on a private network.

Device Name	IP Address	IP address type
DESKTOP-KJE5	192.168.1.77	Private
DESKTOP-KJE5	86.157.52.21	Public
CMNatic-PC	192.168.1.74	Private
CMNatic-PC	86.157.52.21	Public

These two devices will be able to use their private IP addresses to communicate with each other. However, any data sent to the Internet from either of these devices will be identified by the same public IP address.

Public IP addresses are given by your Internet service provider (or ISP) at a monthly fee (your bill)

MAC Addresses

- Devices on a network will all have a physical network interface, which is a microchip board bound on the device's motherboard.
- This network interface is assigned a unique address at the factory it was built at, called a MAC (Media Access Control) address.
- The MAC address is a twelve-character hexadecimal number (a base sixteen numbering system used in computing to represent numbers) split into two's and seperated by a colon. These colons are considered seperators.

Eg. a4:63:F0:85:ac:2d. The first six characters represent the company that made the network interface, and last six is a unique number.

a4:c3:F0:85:ac:2d

- a4:c3:F0 — Vendor who build the network interface (Intel here)
- 85:ac:2d — Unique address of the network interface.

PAGE NO.
DATE : / /

⇒ However, an interesting thing with MAC addresses is that they can be "faked or" "spoofed" in a process known as spoofing.

→ This spoofing occurs when a networked device pretends to identify as another using its MAC address.

When this occurs, it can often break poorly implemented security designs that assume that devices talking on a network are trustworthy.

→ Take the following scenario :-

A firewall is configured to allow any communication going to and from the MAC address of the administrator. If a device were to pretend or "spoof" this MAC address, the firewall would now think that it is receiving communication from the administrator when it isn't.

Local Area Network

PAGE NO.
DATE: / /

→ In reference to networking, when we refer to the term "topology", we are actually referring to the design or look of the network at hand.

STAR topology

→ The main premise of a star topology is that devices are individually connected via a central networking device such as a switch or hub.
This topology is the most commonly found today because of its reliability and scalability - despite the cost.

Any information sent to a device in this topology is sent via the central device to which it connects.

⇒ Advantages And Disadvantages

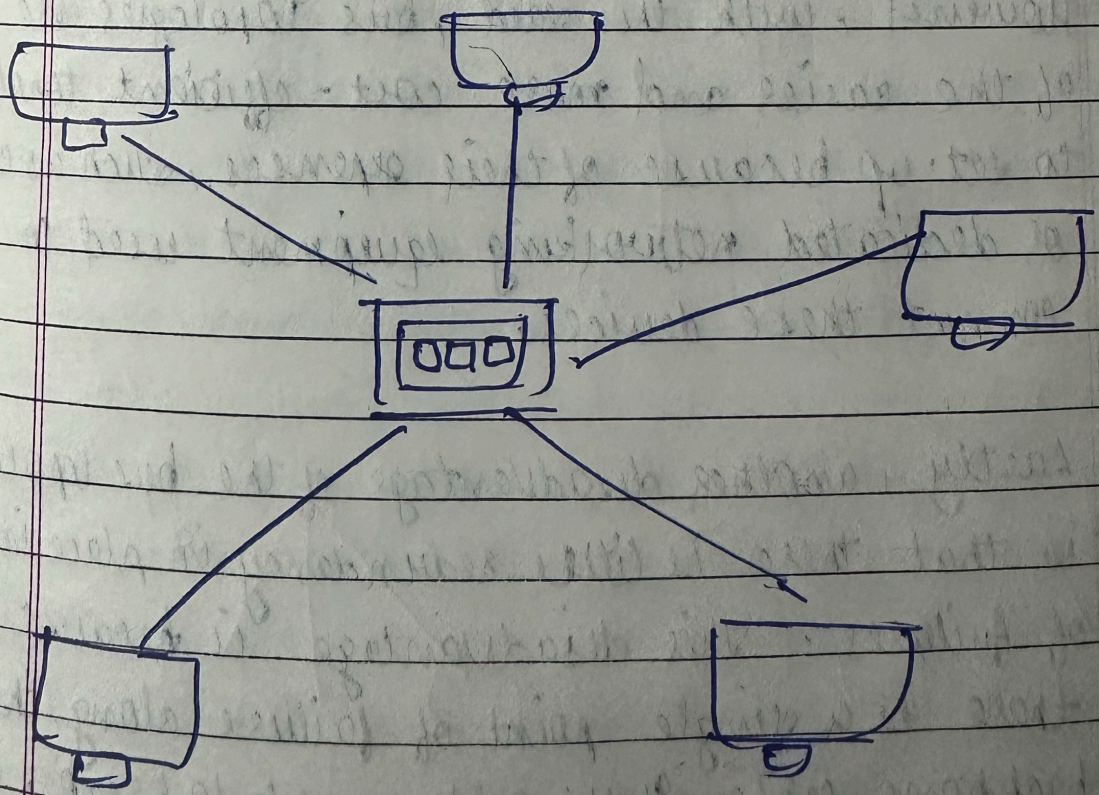
- Because more cabling and the purchase of dedicated networking equipment is required for this topology, it is more expensive than any of the other topologies.

However, despite the added cost, this does provide some significant advantages. For eg.

which means that it is very easy to add more devices as the demand for the network increases.

Unfortunately, the more the network scales, the more maintenance is required to keep the network function. This increase dependence on maintenance can also make troubleshooting faults much harder.

Furthermore, the star topology is still prone to failure - albeit (though reduced).
Eg. - if the centralised hardware that connects devices fails, these devices will no longer be able to send or receive data.
Thankfully, these centralized hardware devices are often robust.



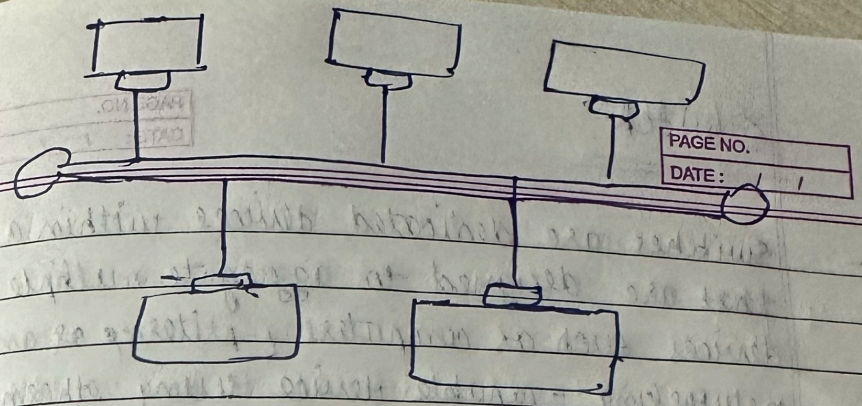
Bus Topology

→ This type of connection relies upon a single connection which is known as a backbone cable

→ Because all data destined for each device travels along the same cable, it is very quickly prone to becoming slow and bottlenecked if devices within the topology are simultaneously requesting data. This bottleneck also results in very difficult troubleshooting because it quickly becomes difficult to identify which device is experiencing issues with data all travelling along the same route.

However, with this said, bus topologies are one of the easies and more cost-efficient topologies to set up because of their expenses, such as cabling of dedicated networking equipment used to connect these devices.

→ Lastly, another disadvantage of the bus topology is that there is little redundancy in place in case of failures. This disadvantage is because there is a single point of failure along the backbone cable. If this cable were to break, device can no longer receive or transmit data along the bus.



PAGE NO.
DATE: /

Ring Topology

- The ring topology (also known as token topology).
- Devices such as computers are connected directly to each other to form a loop, meaning that there is little cabling required and less dependence on dedicated hardware such as within a star topology.

- A ring topology works by sending data across the loop until it reaches the destined device, using other devices along the loop to forward the data. Interestingly, a device will only send received data from another device in this topology if it does not have any to send itself. If the device happens to have data to send, it will send its own data first before sending data from another device.

- Because there is only one direction for data to travel across this topology, it is fairly easy to troubleshoot any faults that arise. However, this is a double-edged sword because it isn't an efficient way of data travelling across a network, as it may have to visit many multiple devices first before reaching the intended device.

A fault such as cable cut, or broken device will result in the entire networking breaking.

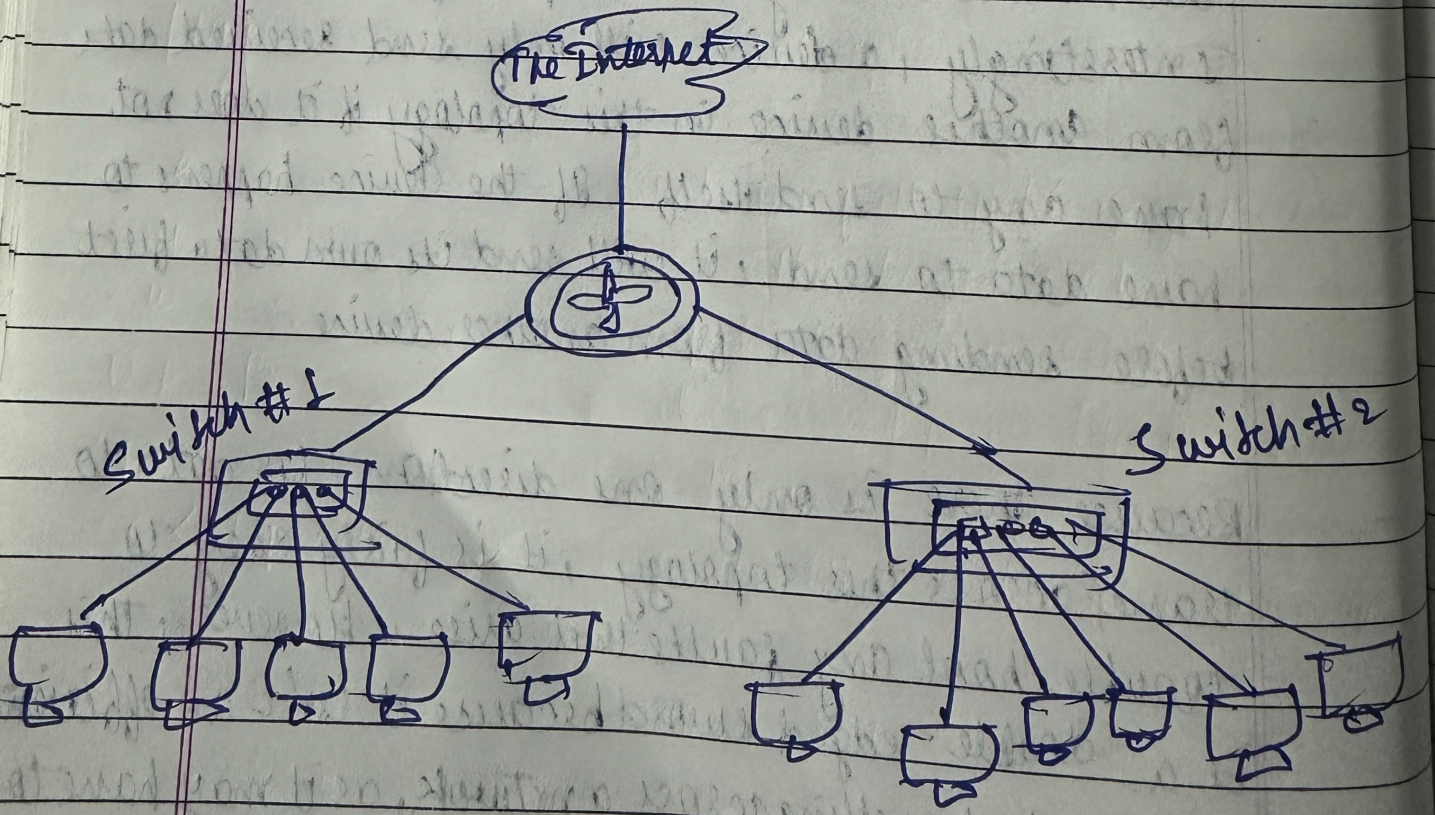
Switch

PAGE NO.
DATE: / /

- Switches are dedicated devices within a network that are designed to aggregate multiple other devices such as computers, printers, or any other networking-capable device using ethernet.

Can be found in larger networks such as businesses, schools, etc.

- Switches are much more efficient than their lesser counterpart (hubs/repeaters). Switches keep track of what devices is connected to which port. This way, when they receive a packet, instead of repeating that packet to every port like a hub would do, it just sends it to the intended targets, thus reducing network traffic.



Router

PAGE NO.
DATE : / /

It's a router's job to connect networks and pass data between them. It does this by using routing.

Routing is the table given to the process of data travelling across networks.
Routing involves creating a path between networks so that this data can be successfully delivered.

Switch

PAGE NO.
DATE: / /

- Switches are dedicated devices within a network that are designed to aggregate multiple other devices such as computers, printers, or any other networking - capable device using ethernet.

Can be found in larger networks such as businesses, schools, etc.

- Switches are much more efficient than their lesser counterpart (hubs/repeaters). Switches keep track of what devices is connected to which port. This way, when they receive a packet, instead of repeating that packet to every port like a hub would do, it just sends it to the intended targets, there reducing network traffic.