COMPUTER NETWORKING

(CET 05201)

UNIT 1

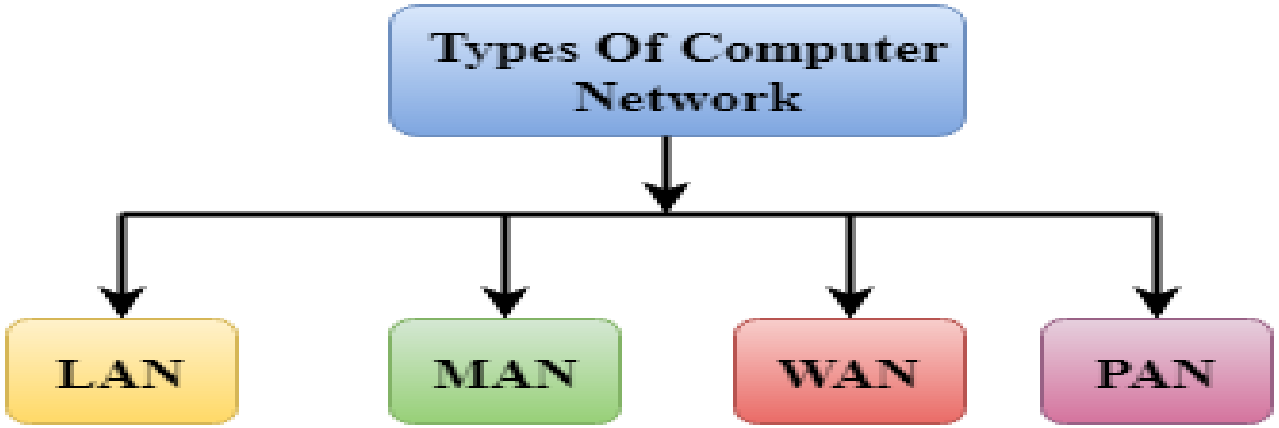
COMPUTER NETWORKING

- **Computer Networking** is the practice of connecting computers together to enable communication and data exchange between them. In general, Computer Network is a collection of two or more computers. It helps users to communicate more easily. In this article, we are going to discuss the basics which everyone must know before going deep into Computer Networking.



Computer Network Types

- A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.
- A computer network can be categorized by their size. A **computer network** is mainly of **four types**:



- LAN(Local Area Network)
- Local Area Network is a group of computers connected to each other in a small area such as building, office.
- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
- It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables.
- The data is transferred at an extremely faster rate in Local Area Network.
- Local Area Network provides higher security.



PAN(PERSONAL AREA NETWORK)

•Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.

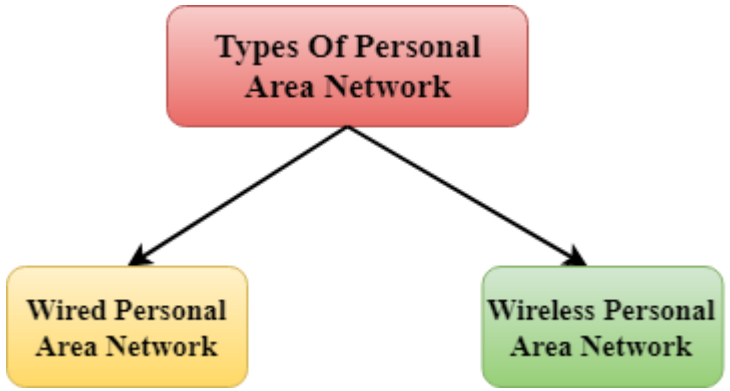
•Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network.

•**Thomas Zimmerman** was the first research scientist to bring the idea of the Personal Area Network.

•Personal Area Network covers an area of **30 feet**.



There are two types of Personal Area Network:



1. Wired Personal Area Network

2. Wireless Personal Area Network

Continue….

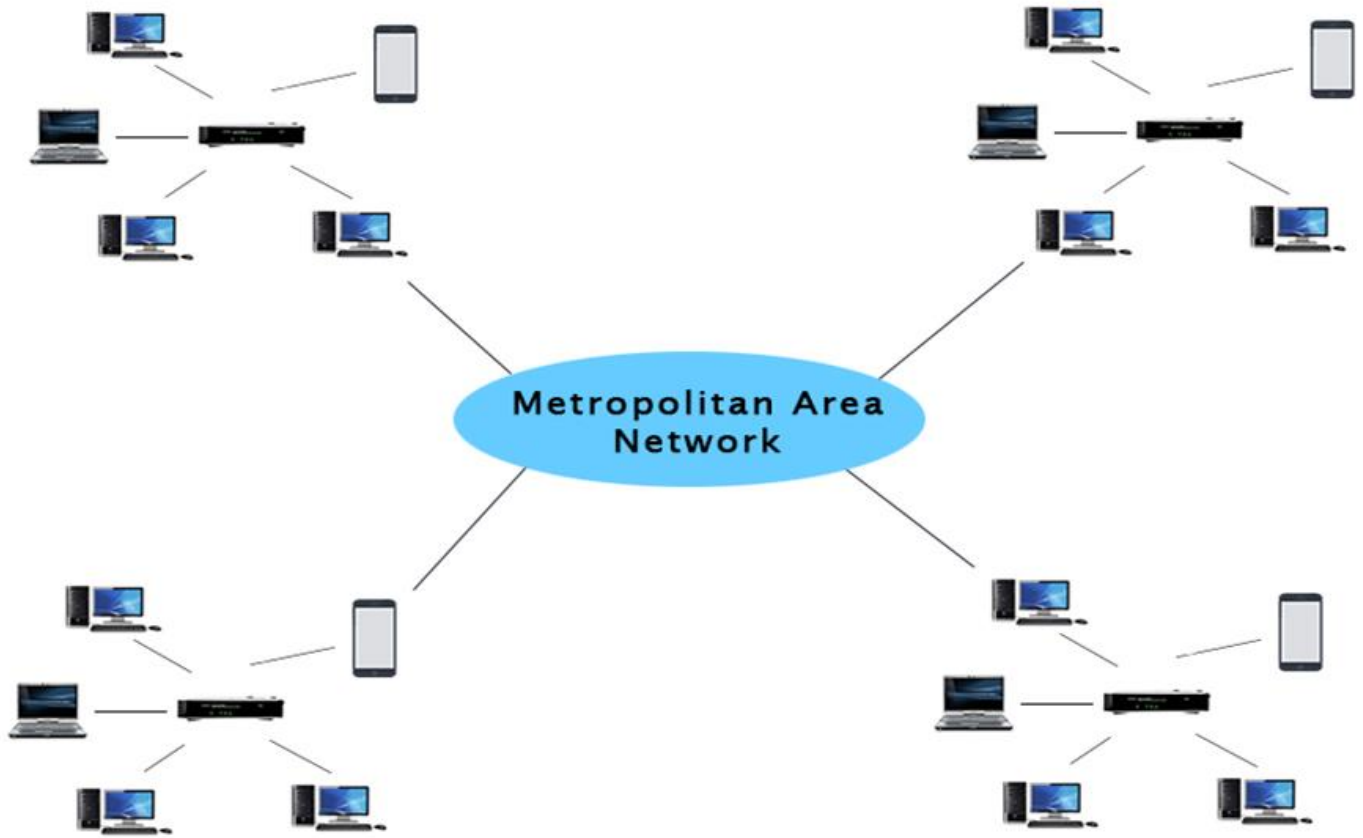
- **Wireless Personal Area Network:** Wireless Personal Area Network is developed by simply using wireless technologies such as WiFi, Bluetooth. It is a low range network.
- **Wired Personal Area Network:** Wired Personal Area Network is created by using the USB.

Examples Of Personal Area Network:

- **Body Area Network:** Body Area Network is a network that moves with a person. **For example**, a mobile network moves with a person. Suppose a person establishes a network connection and then creates a connection with another device to share the information.
- **Offline Network:** An offline network can be created inside the home, so it is also known as a **home network**. A home network is designed to integrate the devices such as printers, computer, television but they are not connected to the internet.

MAN(Metropolitan Area Network)

- A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
- Government agencies use MAN to connect to the citizens and private industries.
- In MAN, various LANs are connected to each other through a telephone exchange line.
- The most widely used protocols in MAN are RS-232, Frame Relay, ATM, ISDN, OC-3, ADSL, etc.
- It has a higher range than Local Area Network(LAN).
-


Metropolitan Area
Network

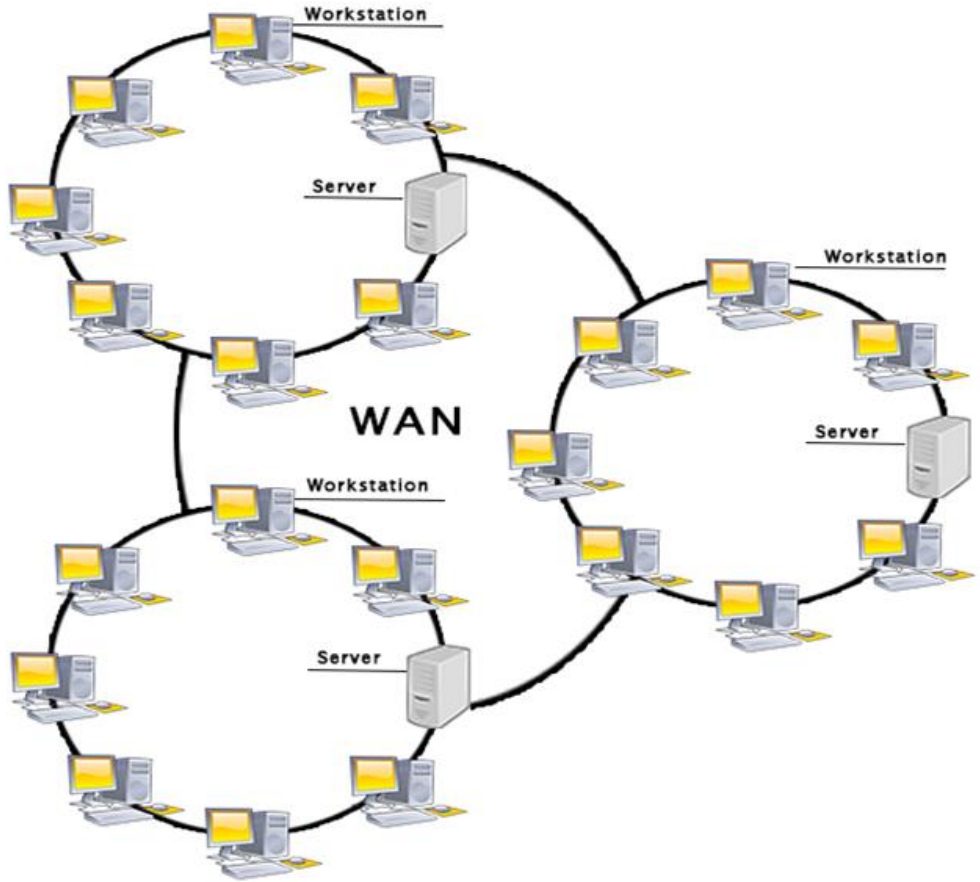
Uses Of Metropolitan Area Network

1. MAN is used in communication between the banks in a city.
2. It can be used in an Airline Reservation.
3. It can be used in a college within a city.
5. It can also be used for communication in the military.

WAN(Wide Area Network)

WAN(Wide Area Network)

- A Wide Area Network is a network that extends over a large geographical area such as states or countries.
- A Wide Area Network is quite bigger network than the LAN.
- A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fibre optic cable or satellite links.
- The internet is one of the biggest WAN in the world.
- A Wide Area Network is widely used in the field of Business, government, and education.


Workstation
Server
Workstation
WAN
Server
Workstation
Server

Examples Of Wide Area Network:

- **Mobile Broadband:** A 4G network is widely used across a region or country.
- **Last mile:** A telecom company is used to provide the internet services to the customers in hundreds of cities by connecting their home with fiber.
- **Private network:** A bank provides a private network that connects the 44 offices. This network is made by using the telephone leased line provided by the telecom company.

Advantages Of Wide Area Network

- Following are the advantages of the Wide Area Network:
- **Geographical area:** A Wide Area Network provides a large geographical area. Suppose if the branch of our office is in a different city then we can connect with them through WAN. The internet provides a leased line through which we can connect with another branch.
- **Centralized data:** In case of WAN network, data is centralized. Therefore, we do not need to buy the emails, files or back up servers.
- **Get updated files:** Software companies work on the live server. Therefore, the programmers get the updated files within seconds.
- **Exchange messages:** In a WAN network, messages are transmitted fast. The web application like Facebook, Whatsapp, Skype allows you to communicate with friends.
- **Sharing of software and resources:** In WAN network, we can share the software and other resources like a hard drive, RAM.
- **Global business:** We can do the business over the internet globally.
- **High bandwidth:** If we use the leased lines for our company then this gives the high bandwidth. The high bandwidth increases the data transfer rate which in turn increases the productivity of our company.

Disadvantages of Wide Area Network

- The following are the disadvantages of the Wide Area Network:
- **Security issue:** A WAN network has more security issues as compared to LAN and MAN network as all the technologies are combined together that creates the security problem.
- **Needs Firewall & antivirus software:** The data is transferred on the internet which can be changed or hacked by the hackers, so the firewall needs to be used. Some people can inject the virus in our system so antivirus is needed to protect from such a virus.
- **High Setup cost:** An installation cost of the WAN network is high as it involves the purchasing of routers, switches.
- **Troubleshooting problems:** It covers a large area so fixing the problem is difficult.

Basic Terminologies of Computer Networks

- **Network:** A network is a collection of computers and devices that are connected together to enable communication and data exchange.
- **Nodes:** Nodes are devices that are connected to a network. These can include computers, Servers, Printers, Routers, Switches, and other devices.
- **Protocol:** A protocol is a set of rules and standards that govern how data is transmitted over a network. Examples of protocols include TCP/IP, HTTP, and FTP.
- **Topology:** Network topology refers to the physical and logical arrangement of nodes on a network. The common network topologies include bus, star, ring, mesh, and tree.
- **Service Provider Networks:** These types of Networks give permission to take Network Capacity and Functionality on lease from the Provider. Service Provider Networks include Wireless Communications, Data Carriers, etc.
- **IP Address**: An IP address is a unique numerical identifier that is assigned to every device on a network. IP addresses are used to identify devices and enable communication between them.
- **DNS:** The Domain Name System (DNS) is a protocol that is used to translate human-readable domain names (such as www.google.com) into IP addresses that computers can understand.
- **Firewall:** A firewall is a security device that is used to monitor and control incoming and outgoing network traffic. Firewalls are used to protect networks from unauthorized access and other security threats

NETWORK TOPOLOGY

- The arrangement of a network that comprises nodes and connecting lines via sender and receiver is referred to as **Network Topology**.

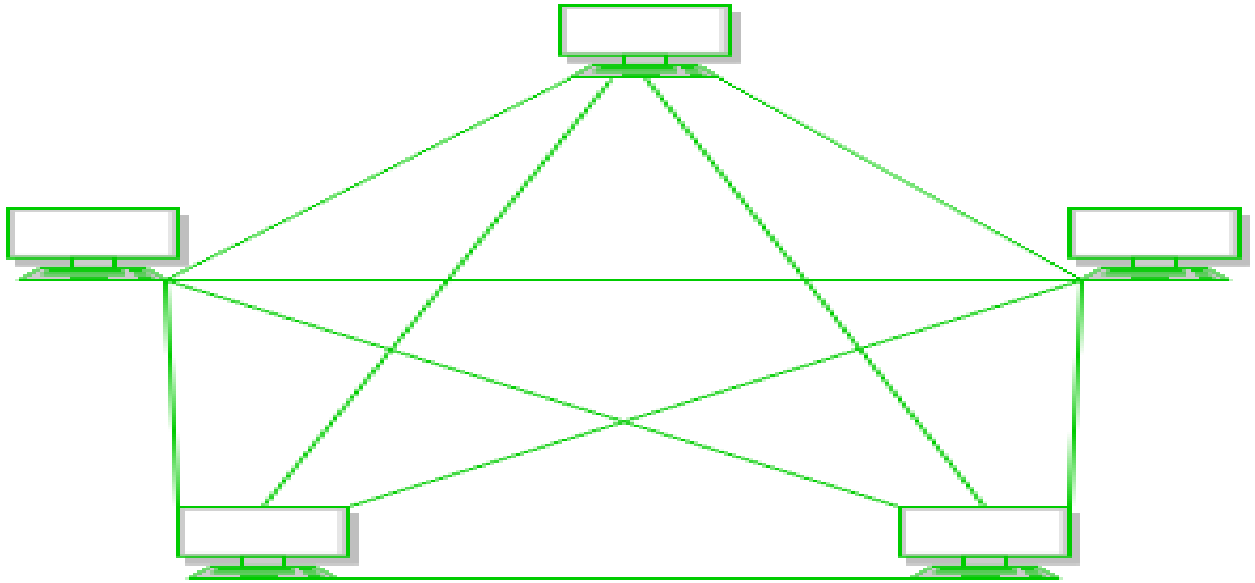
TYPES OF NETWORK TOPOLOGY

The various network topologies are:

- Mesh Topology
- Star Topology
- Bus Topology
- Ring Topology
- Tree Topology
- Hybrid Topology

MESH TOPOLOGY

- In a mesh topology, every device is connected to another device via a particular channel. Every device is connected to another via dedicated channels. These channels are known as links. In Mesh Topology, the protocols used are AHCP (Ad Hoc Configuration Protocols), DHCP (Dynamic Host Configuration Protocol), etc.



Advantages of Mesh Topology

- Communication is very fast between the nodes.
- Mesh Topology is robust.
- The fault is diagnosed easily. Data is reliable because data is transferred among the devices through dedicated channels or links.
- Provides security and privacy.

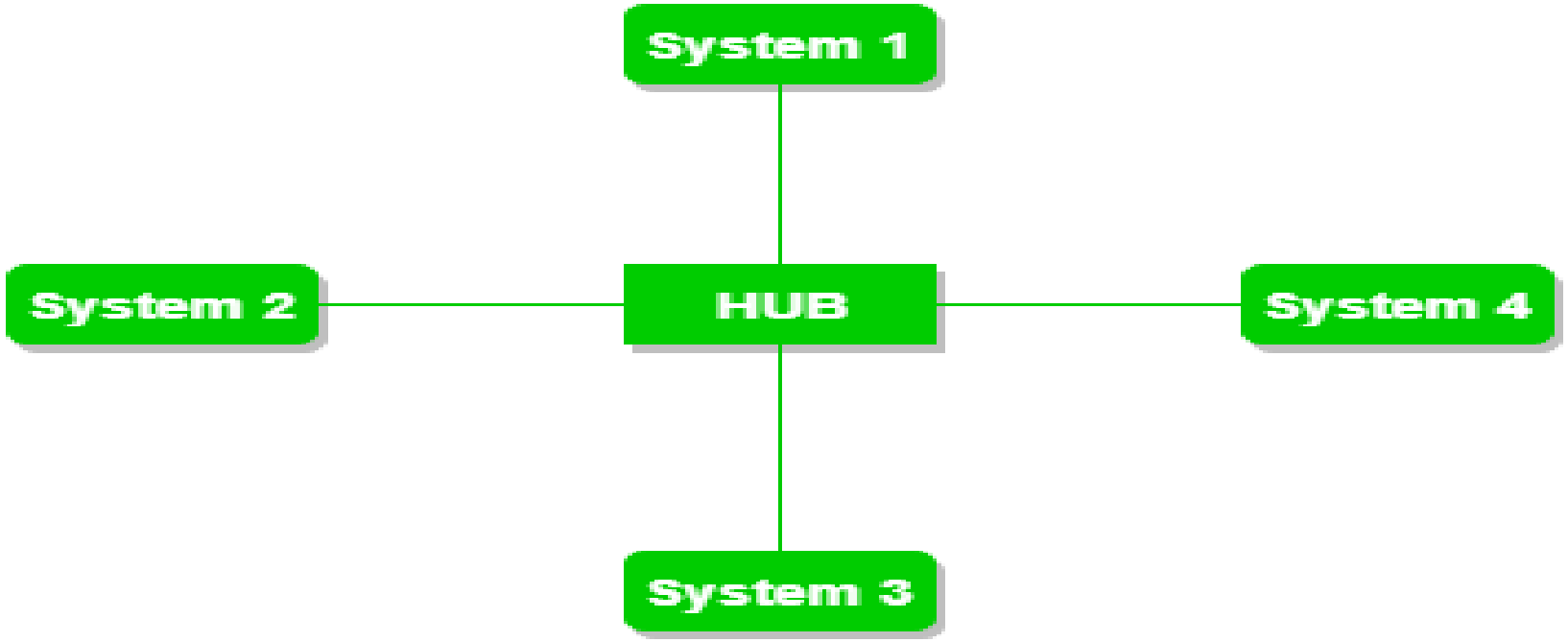
Drawbacks of Mesh Topology

- Installation and configuration are difficult.
- The cost of cables is high as bulk wiring is required, hence suitable for less number of devices.
- The cost of maintenance is high.

A common example of mesh topology is the internet backbone, where various internet service providers are connected to each other via dedicated channels. This topology is also used in military communication

STAR TOPOLOGY

- In Star Topology, all the devices are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node.



Advantages of Star Topology

- **Efficient troubleshooting:** Troubleshooting is quite efficient in a star topology as compared to bus topology. In a bus topology, the manager has to inspect the kilometers of cable. In a star topology, all the stations are connected to the centralized network. Therefore, the network administrator has to go to the single station to troubleshoot the problem.
- **Network control:** Complex network control features can be easily implemented in the star topology. Any changes made in the star topology are automatically accommodated.
- **Limited failure:** As each station is connected to the central hub with its own cable, therefore failure in one cable will not affect the entire network.
- **Familiar technology:** Star topology is a familiar technology as its tools are cost-effective.
- **Easily expandable:** It is easily expandable as new stations can be added to the open ports on the hub.
- **Cost effective:** Star topology networks are cost-effective as it uses inexpensive coaxial cable.
- **High data speeds:** It supports a bandwidth of approx 100Mbps. Ethernet 100BaseT is one of the most popular Star topology networks.

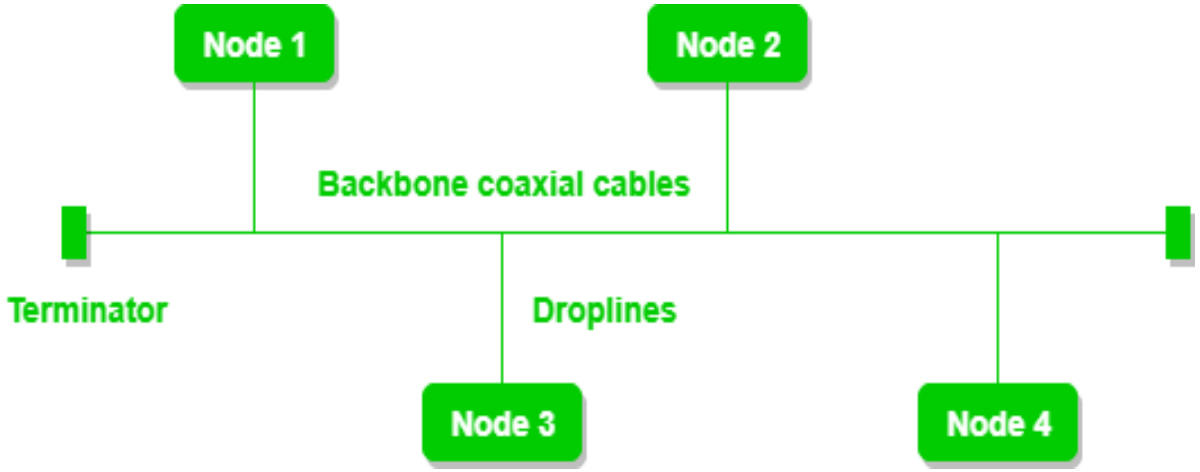
Drawbacks of Star Topology

- **A Central point of failure:** If the central hub or switch goes down, then all the connected nodes will not be able to communicate with each other.
- **Cable:** Sometimes cable routing becomes difficult when a significant amount of routing is required.

•The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.Each node is either connected to the backbone cable by drop cable or directly connected to the backbone cable.

•When a node wants to send a message over the network, it puts a message over the network. All the stations available in the network will receive the message whether it has been addressed or not.

•The bus topology is mainly used in 802.3 (ethernet) and 802.4 standard networks.The configuration of a bus topology is quite simpler as compared to other topologies.



BUS TOPOLOGY

The most common access method of the bus topologies is **CSMA** (Carrier Sense Multiple Access).

- **CSMA:** It is a media access control used to control the data flow so that data integrity is maintained, i.e., the packets do not get lost.

- **Advantages of Bus Topology**
- **Low-cost cable:** In bus topology, nodes are directly connected to the cable without passing through a hub. Therefore, the initial cost of installation is low.
- **Moderate data speeds:** Coaxial or twisted pair cables are mainly used in bus-based networks that support upto 10 Mbps.
- **Familiar technology:** Bus topology is a familiar technology as the installation and troubleshooting techniques are well known, and hardware components are easily available.
- **Limited failure:** A failure in one node will not have any effect on other nodes.

Drawbacks of Bus Topology

- **Extensive cabling:** A bus topology is quite simpler, but still it requires a lot of cabling.
- **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
- **Signal interference:** If two nodes send the messages simultaneously, then the signals of both the nodes collide with each other.
- **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
- **Attenuation:** Attenuation is a loss of signal leads to communication issues. Repeaters are used to regenerate the signal.

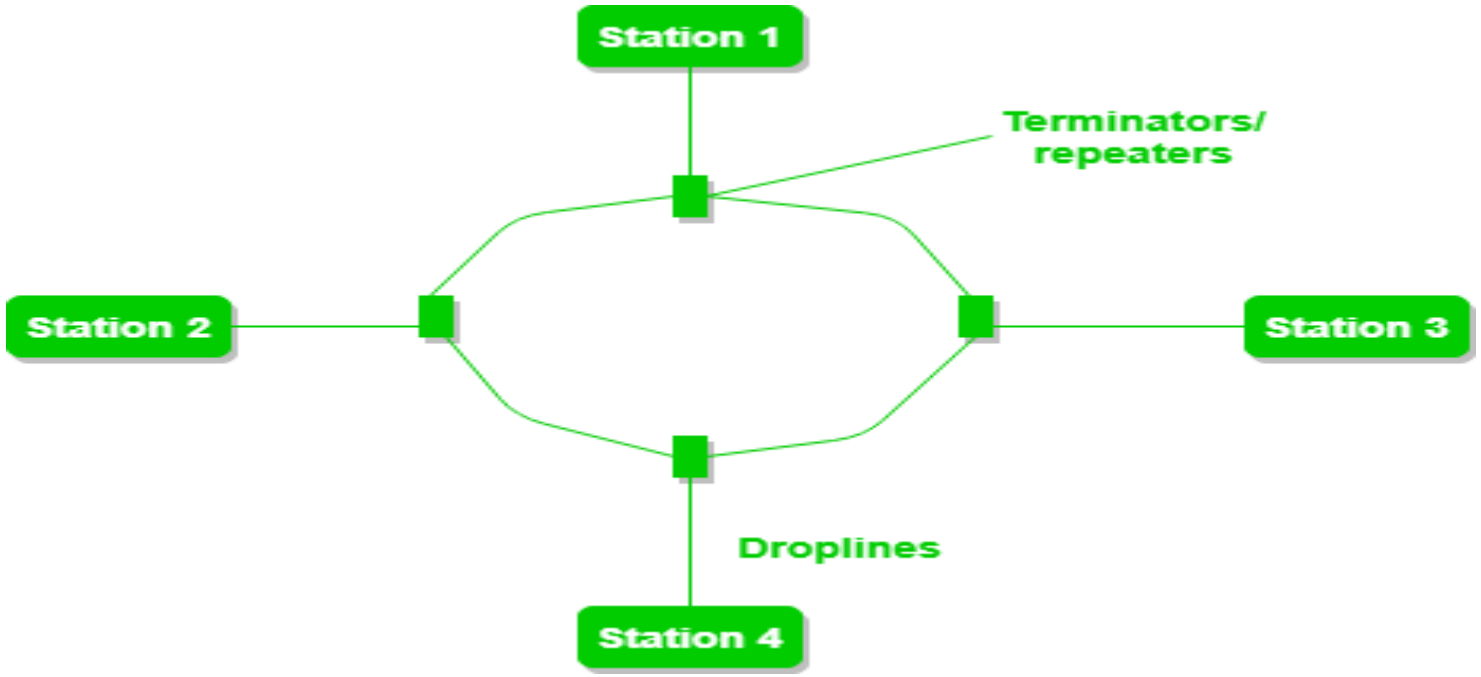
RING TOPOLOGY

- In a Ring Topology, it forms a ring connecting devices with exactly two neighboring devices. A number of repeaters are used for Ring topology with a large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.

- The data flows in one direction, i.e. it is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology. In-Ring Topology, the Token Ring Passing protocol is used by the workstations to transmit the data.

A ring topology comprises 4 stations connected with each forming a ring. The most common access method of ring topology is token passing.

- **Token passing:** It is a network access method in which a token is passed from one node to another node.
- **Token:** It is a frame that circulates around the network.



OPERATIONS OF RING TOPOLOGY

- One station is known as a **monitor** station which takes all the responsibility for performing the operations.
- To transmit the data, the station has to hold the token. After the transmission is done, the token is to be released for other stations to use.
- When no station is transmitting the data, then the token will circulate in the ring.
- There are two types of token release techniques: **Early token release** releases the token just after transmitting the data and **Delayed token release** releases the token after the acknowledgment is received from the receiver.

Advantages of Ring Topology

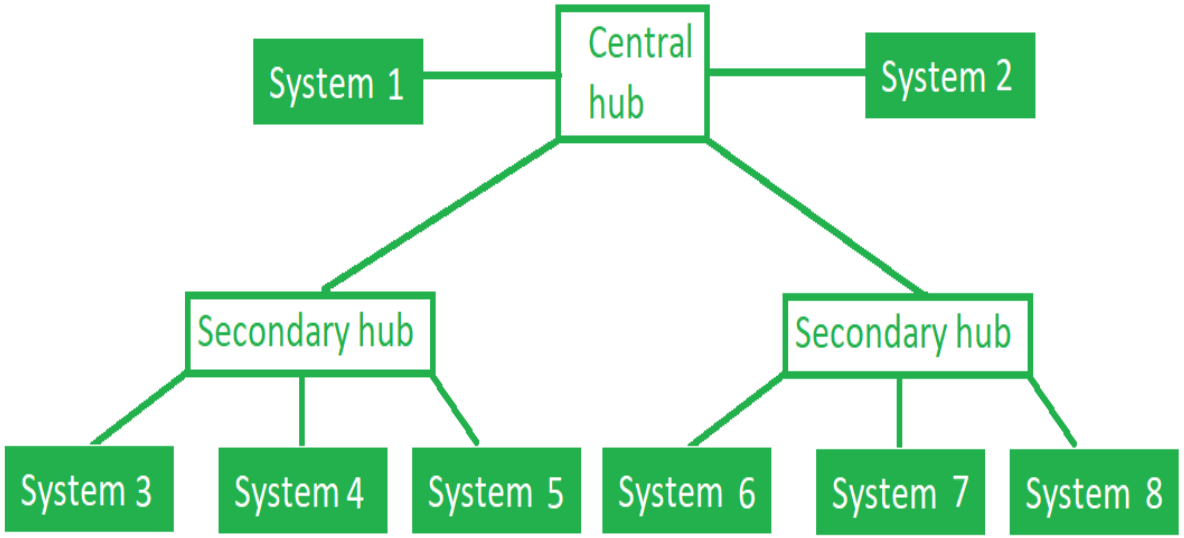
- The data transmission is high-speed.
- The possibility of collision is minimum in this type of topology.
- Cheap to install and expand.
- It is less costly than a star topology.

Drawbacks of Ring Topology

- The failure of a single node in the network can cause the entire network to fail.
- Troubleshooting is difficult in this topology.
- The addition of stations in between or the removal of stations can disturb the whole topology.
- Less secure.

TREE TOPOLOGY

- This topology is the variation of the Star topology. This topology has a hierarchical flow of data. In Tree Topology, protocols like DHCP and SAC (Standard Automatic Configuration) are used.



Continue…….

- In this, the various secondary hubs are connected to the central hub which contains the repeater. This data flow from top to bottom i.e. from the central hub to the secondary and then to the devices or from bottom to top i.e. devices to the secondary hub and then to the central hub. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes.

Advantages of Tree Topology

- It allows more devices to be attached to a single central hub thus it decreases the distance that is traveled by the signal to come to the devices.
- It allows the network to get isolated and also prioritize from different computers.
- We can add **new devices to the existing network.**
- **Error detection** and **error correction** are very easy in a tree topology.

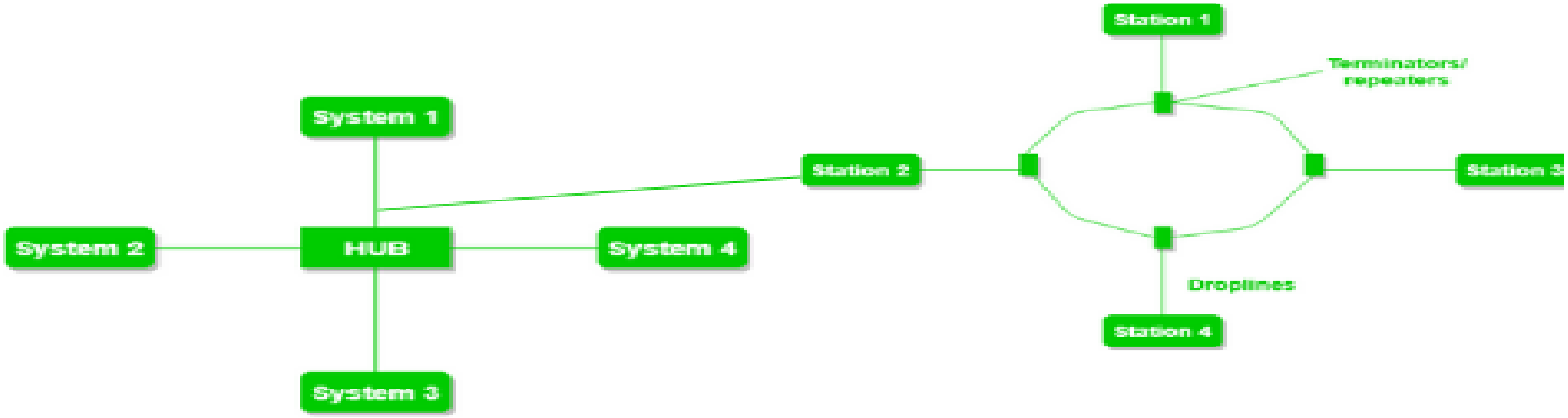
Drawbacks of Tree Topology

- If the central hub gets fails the entire system fails.
- The cost is high because of the cabling.
- If new devices are added, it becomes difficult to reconfigure.

A common example of a tree topology is the hierarchy in a large organization. At the top of the tree is the CEO, who is connected to the different departments or divisions (child nodes) of the company. Each department has its own hierarchy, with managers overseeing different teams (grandchild nodes). The team members (leaf nodes) are at the bottom of the hierarchy, connected to their respective managers and departments.

HYBRID TOPOLOGY

- This topological technology is the combination of all the various types of topologies we have studied above. Hybrid Topology is used when the nodes are free to take any form. It means these can be individuals such as Ring or Star topology or can be a combination of various types of topologies seen above. Each individual topology uses the protocol that has been discussed earlier.



Advantages of Hybrid Topology

- This topology is **very flexible**.
- The size of the network can be easily expanded by **adding new devices.**

Drawbacks of Hybrid Topology

- It is challenging **to design the architecture** of the Hybrid Network.
- **Hubs** used in this topology are **very expensive.**
- The infrastructure cost is very high as a hybrid network **requires a lot of cabling and network devices**

A common example of a hybrid topology is a university campus network. The network may have a backbone of a star topology, with each building connected to the backbone through a switch or router. Within each building, there may be a bus or ring topology connecting the different rooms and offices. The wireless access points also create a mesh topology for wireless devices. This hybrid topology allows for efficient communication between different buildings while providing flexibility and redundancy within each building.

NETWORK DEVICES

- Network devices, also known as networking hardware, are physical devices that allow hardware on a computer network to communicate and interact with one another.

For example

- Repeater,
- Hub,
- Bridge,
- Switch,
- Routers,
- Gateway,
- Brouter
- NIC, etc.

1.Repeater

- A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they not only amplify the signal but also regenerate it. When the signal becomes weak, they copy it bit by bit and regenerate it at its star topology connectors connecting following the original strength. It is a 2-port device

2. Hub

- A hub is a basically multi-port repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, the collision domain of all hosts connected through Hub remains one. Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage

TYPES OF HUB

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.

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.

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. Bridge

- A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of the source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

TYPES OF BRIDGES

Transparent Bridges

- These are the bridge in which the stations are completely unaware of the bridge's existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and bridge learning.

Source Routing Bridges

- In these bridges, routing operation is performed by the source station and the frame specifies which route to follow. The host can discover the frame by sending a special frame called the discovery frame, which spreads through the entire network using all possible paths to the destination.

4. Switch

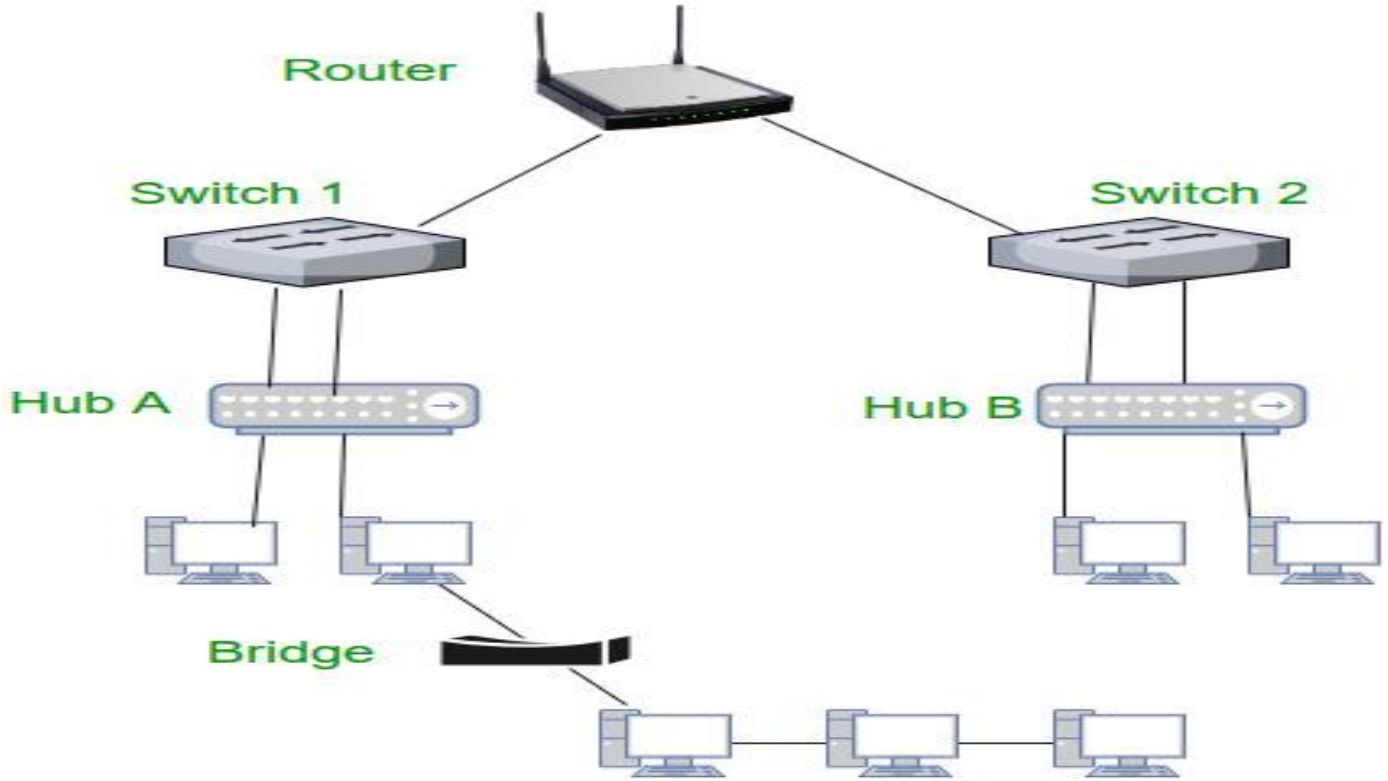
- A switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only. In other words, the switch divides the collision domain of hosts, but the broadcast domain remains the same.

5. NIC

- NIC or network interface card is a network adapter that is used to connect the computer to the network. It is installed in the computer to establish a LAN. It has a unique id that is written on the chip, and it has a connector to connect the cable to it. The cable acts as an interface between the computer and the router or modem. NIC card is a layer 2 device which means that it works on both the physical and data link layers of the network model.

6. Routers

- A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs and have a dynamically updating routing table based on which they make decisions on routing the data packets. The router divides the broadcast domains of hosts connected through it.



7. Gateway

- A gateway, as the name suggests, is a passage to connect two networks that may work upon different networking models. They work as messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switches or routers. A gateway is also called a protocol converter.

8. Brouter

- It is also known as the bridging router is a device that combines features of both bridge and router. It can work either at the data link layer or a network layer. Working as a router, it is capable of routing packets across networks and working as the bridge, it is capable of filtering local area network traffic.

Sub-Netting

A **subnet mask** is used in a process known as subnetting, in which a large network is divided into smaller networks. It's like dividing a network into several contiguous network groups, and each group is known as a subnet.

Moreover, this process is implemented to reduce the wastage of IP addresses due to classful addressing.

A **subnet mask** is used to determine the network address and host address:

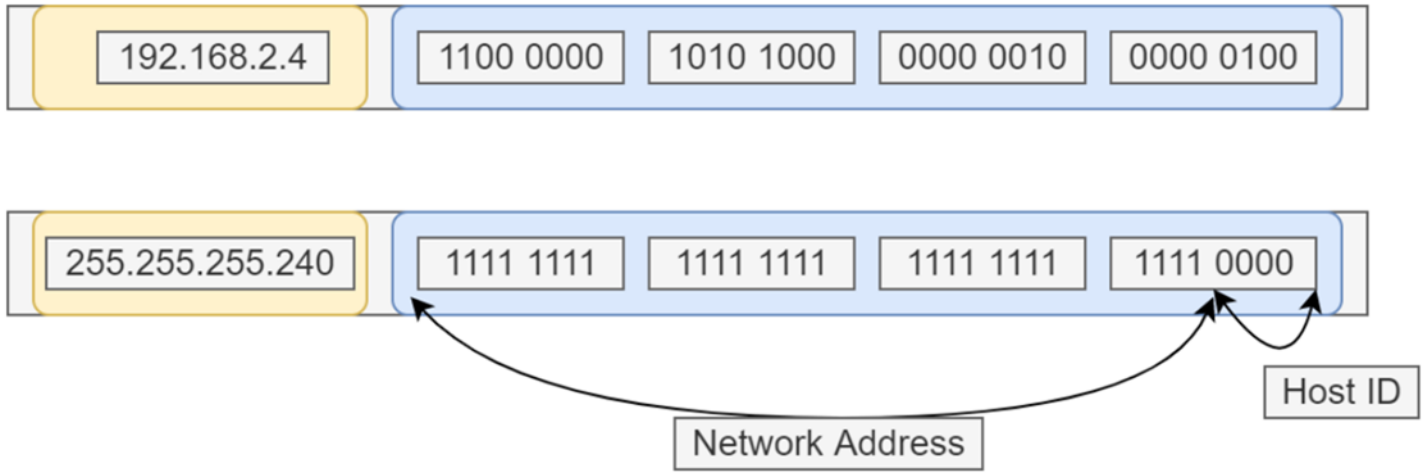
Class	Default Subnet mask
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Sub-netting is a division of the network in to small parts so as to simplify troubleshooting, make better use of IP address and Security purposes.

Calculating network and broadcast addresses using a subnet mask.

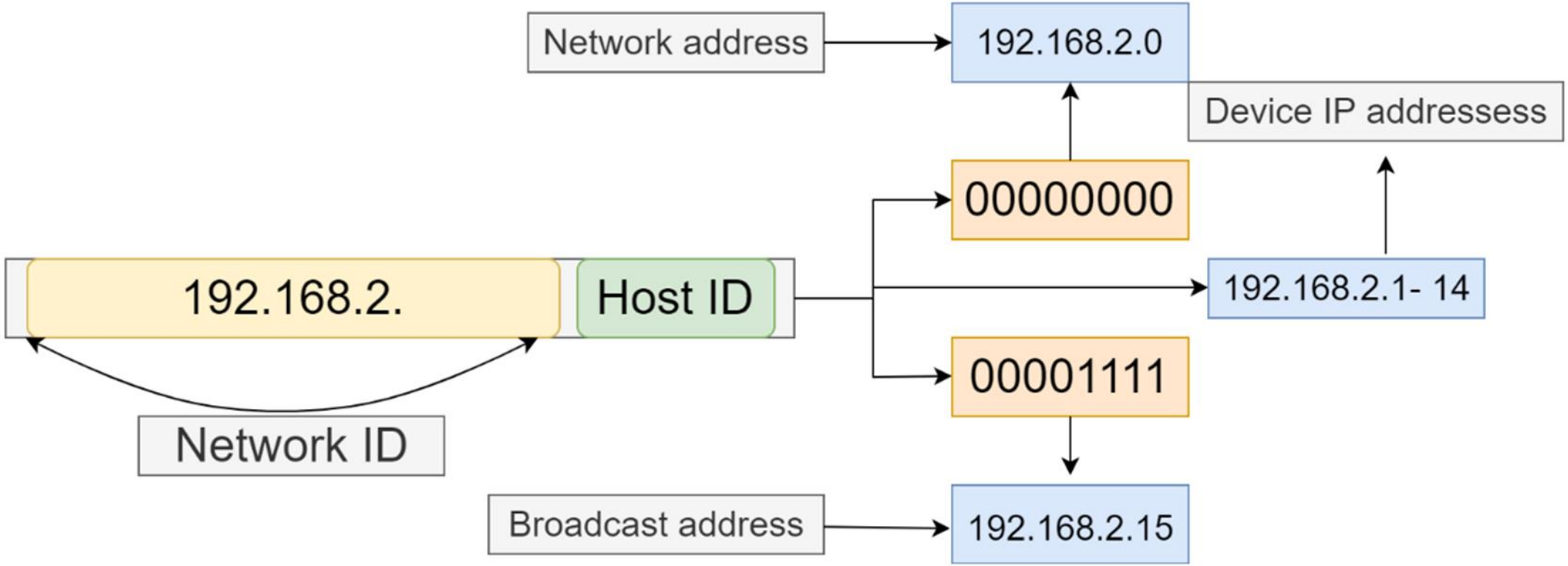
Given: IP address is 192.168.2.4 and the subnet mask is 255.255.255.240.

The first step is to write down the IP address and subnet mask in binary:



Bits in the subnet mask which are 1 denotes the network address. Similarly, the bits which are 0 will be used for the broadcast address.

In this example, we can see that the last 4 bits of the subnet mask are 0. Hence, this means we can connect 14 devices (192.168.2.1 - 192.168.2.14) and the broadcast IP address will be 192.168.2.15. Therefore, the network address will be 192.168.2.0



Hence, we can also rewrite the above IP address: 192.168.2.4/28. Here, 28 refers to the 28 bits of the subnet mask, *which are 1*.

Moreover, the IP address 192.168.2.4 belongs to class C. Hence, we know that in class C, the first 24 bits of the IP address is used for the network address, and the rest is used for the host address. In contrast, *there's a case in subnet mask where network addresses can exceed 24 bits*.

The division of the first 24 bits for network and host addresses is the default configuration for the class C IP address.

Hence, we can change that by changing the number of 1 in the subnet mask. Moreover, we know that the *default subnet mask for class C is 255.255.255.0*.

Example

We can change some bits of the subnet mask:

IP Address = 192.168.2.4 = 1100 0000. 1010 1000. 0000 0010. 0000 0100

Subnet mask = 255.255.255.224 = 1111 1111. 1111 1111. 1111 1111. 1110 0000



Hence, the IP address with this subnet mask will be in a different network. This is the way we can divide a network using the subnet mask. Therefore, now we can rewrite the IP address as 192.168.2.4/27.

Subnet Mask

In the IPV4 addressing scheme, a 32-bits number is selected for any IP address. The IP address is divided into the following two parts:

- Network Address(network identification, network ID, net Id or netid field)
- Host Address (host identification, host ID, or hostid field)

The network address is common to all hosts within a given network, the network designer assigns a unique network address to a given network, and the hosts are then assigned values for the host part of the IP address.

This setup results in all hosts within the network having a common network address prefix.

The number of bits used in the network address prefix depends on the format of the IP address.

Class A address format, 8 bits are used for the network address, and 24 bits are used for the host address.

Class B address format, 16 bits are used for the network address, and 16 bits are used for the host address.

Class C address format, 24 bits are used for the network address, and 8 bits are used for the host address.

The advantage of using a two-part scheme of network address and host address for IP address has the advantage of minimizing the number of entries in a routers' routing table.

Instead of having routing table entry for each host on a network, you can now summarize all the host in a network by using a single routing table entry.

This routing table entry contains only the network address part, which is the common prefix for all hosts in the network.

A subnet mask is a 32-bit number created by setting host bits to all 0s and setting network bits to all 1s. In this way, the subnet mask separates the IP address *into* the network and host addresses.

The “255” address is always assigned to a broadcast address, and the “0” address is always assigned to a network address.

Neither can be assigned to hosts, as they are reserved for these special purposes.

When organizations need additional subnetworking, subnetting divides the host element of the IP address further into a subnet.

The goal of subnet masks are simply to enable the subnetting process. The phrase “mask” is applied because the subnet mask essentially uses its own 32-bit number to mask the IP address.

IP Address and Subnet Mask

A 32-bit IP address uniquely identifies a single device on an IP network. The 32 binary bits are divided into the host and network sections by the subnet mask but they are also broken into four 8-bit octets.

Because binary is challenging, we convert each octet so they are expressed in dot decimal. This results in the characteristic dotted decimal format for IP addresses for example, 172.16.254.1.

The range of values in decimal is 0 to 255 because that represents 00000000 to 11111111 in binary.

IP Address Classes and Subnet Masks

A **Class A** subnet mask reflects the network portion in the first octet and leaves octets 2, 3, and 4 for the network manager to divide into hosts and subnets as needed.

Class A is for networks with more than 65,536 hosts.

A **Class B** subnet mask claims the first two octets for the network, leaving the remaining part of the address, the 16 bits of octets 3 and 4, for the subnet and host part.

Class B is for networks with 256 to 65,534 hosts.

A **Class C** subnet mask, the network portion is the first three octets with the hosts and subnets in just the remaining 8 bits of octet 4.

Class C is for smaller networks with fewer than 254 hosts.

Class A, B, and C networks have natural masks, or default subnet masks:

Class A: 255.0.0.0

Class B: 255.255.0.0

Class C: 255.255.255.0

You can determine the number and type of IP addresses any given local network requires based on its default subnet mask.

How Does Subnetting Work?

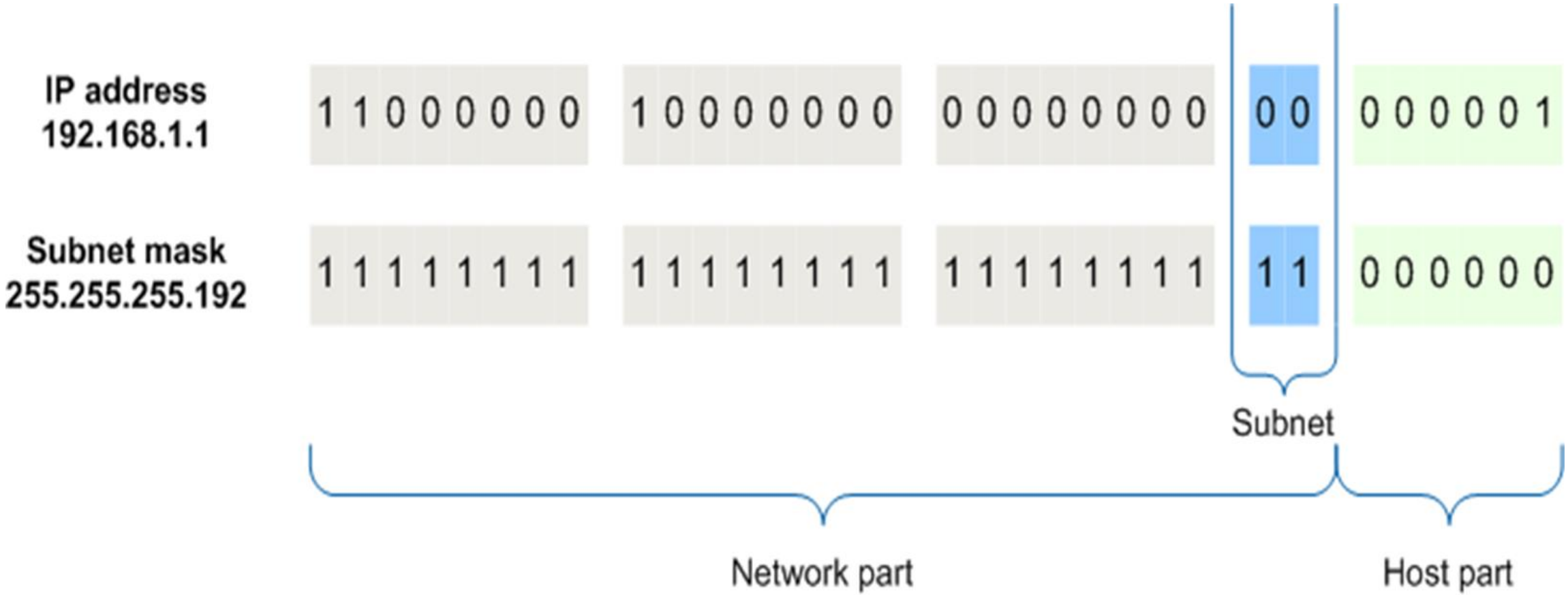
Subnetting is the technique for logically partitioning a single physical network into multiple smaller sub-networks or subnets.

Subnetting enables an organization to conceal network complexity and reduce network traffic by adding subnets without a new network number.

When a single network number must be used across many segments of a local area network (LAN), subnetting is essential.

The benefits of subnetting include:

i. Reducing broadcast volume and thus network traffic
ii. Enabling work from home
iii. Allowing organizations to surpass LAN constraints such as maximum number of hosts


IP address
192.168.1.1
1 1 0 0 0 0 0 0
1 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0
0 0
0 0 0 0 0 1
Subnet mask
255.255.255.192
1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1
1 1
0 0 0 0 0 0
Subnet
Network part
Host part

Formulas used in Different Calculations

Number of Hosts $= 2^n$-2

Where n is number of *remaining bits to make total of 32-bits*

Number of IPs $= 2^n$

Where n is the number of *remaining bits to make total of 32-bits*

Number of Networks $= 2^n$

Where n is number of *borrowed bits after the default of 24-bits for network address of class C.*

NOTE: The number of Hosts are the number of usable IPs. Meaning, after deduction of the network address and broadcast address the remaining will be the usable IPs/ Hosts.

Example

Use the given IP address 192.55.12.4/28 Find the following

i. Subnet mask
ii. Number of IPs
iii. Number of Hosts
iv. Network address
v. Broadcast address
vi. Number of Network(s)

Use the given IP address 192.55.12.6 and the subnet mask 255.255.255.252 Find the following

i. Number of IPs
ii. Number of Hosts
iii. Network address
iv. Broadcast address
v. Number of Network(s)
vi. Rewrite the IP address

Definition of Terms

Network ID is the First IP address in each Sub-network

Broadcast IP is the Last IP address in each sub-network

First Host IP is the address after the Network ID

Last Host IP is the address before the Broadcast IP

Next Network is the Next ID of the next sub-network

Number of IP address number of IP in each sub network

CIDR(classless inter-Domain Routing) an IP address allocation method that improve data routing effiency in the internet i.e. 192.55.12.4/28