

# Study Unit 6

# IP Addressing

## Study Session Outline

- IP addressing
- IP Classes
- Forms of IP

## Study Session

### Duration

This Study Session requires a 2 hours of formal study time.

You may spend an additional 2-3 hours for revision

## Introduction

This Study Unit introduces the various classes and versions of the IP addressing. It also carefully presents examples of IP address division known as subnets. A flash of binary number conversion is intended to be treated.

## Learning Outcomes of Study Unit 6

Upon completion of this study unit, you should be able to:

- 6.1 Explain the structure if IPv4 and IPv6 addresses.
- 6.2 List the classes of IPv4 address and state their uses.
- 6.3 Demonstrate how to subnet a network.
- 6.4 Illustrate the different types of network topology.
- 6.5 Design simple topologies for Local Area Networks (LAN)

## Terminologies

IP	Internet Protocols
Subnet	Sub Network addressing

## 6.1 IP ADDRESSING

Managing Internet Protocol (IP) Addresses is an integral part of Computer Networks. It is a global or private identifier that grants a computer access on a Network.



*What layer in the OSI Model manages IP Addressing?*

As we said in layer architecture, every computer/device in a network (public or private) must have an IP address to send and receive messages.

An IP address can be defined as a numerical representation that uniquely identifies a computer/device in a network. A device can be a smartphone or any digital device that can connect to a computer network.

### 6.1.1 IPv4 and IPv6

IP addresses are divided in version 4 (IPv4) and version 6 (IPv6). IP addressing started with version 4 which uses 32-bit number structure. Because of the depletion of IPv4 addresses, IPv6 was developed by the Internet Engineering Taskforce (IETF) and uses 128 bits number structure. The two versions are currently in use.

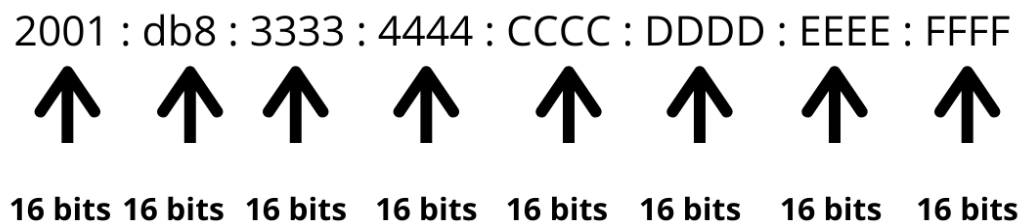
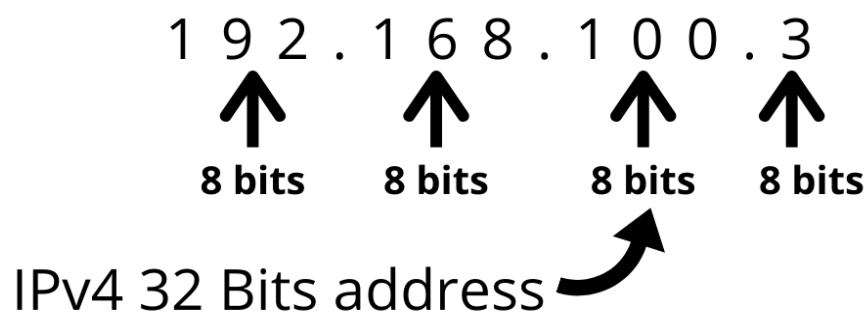


The computer recognizes numbers, alphabets, images, audio and video in binary digits. These are numbers represented in '0' and '1'.  
For e.g., 1001010 is a binary digit.



Which of these numbers is not a NOT binary number?

- A. 100101101
- B. 101
- C. 10
- D. 103



IPv6 128 Bits address

*Figure 1: IP in Bits*

## Ipv4

Ipv4 is made up of 32-bit number structure. The total number of IPv4 addresses are  $2^{32} = 4,294,967,296$ . The address space is limited to 4,294,967,296 IP addresses; this was why Ipv6 was developed.

Among these billions of addresses, 18 million addresses were reserved for private networks, while 270 million was reserved for multicast addresses.

## IPv4 Address Structure

The IPv4 32-bit address is made up of four 8 bits that is represented in decimal form. IPv4 addresses have one thing in common, they are separated by dots. For e.g., 192.168.1.1 is seen as 11000000.10101000.00000001.00000001 by the computer. These numbers that are in '0s' and '1' are called binary numbers, base two numbers or binary digits.



*Do you know how to convert numbers to binary base 2?  
Try and convert 158 to binary number*

Conversion of 158 to binary digits

2	→	158		
2	→	79	R	0
2	→	39	R	1
2	→	19	R	1
2	→	9	R	1
2	→	4	R	1
2	→	2	R	0
2	→	1	R	0
	→	0	R	1

Count upwards

*The answer is 10011110*

*Figure 2: Conversion of 150 to binary digits*

E.g., 10.6.111.231 is an IP address. The computer takes 10.6.111.231 which is in decimal (base 10) and converts it to machine-readable format in base 2. This is how the computer sees the above IP address

00001010.00000110.01101111.11100111



*The network administrator assigned 172.168.1.196 as your IP address, convert the IP address to binary digits.*

## Classes of IPv4 Addresses

This is commonly referred to as classful network addressing. The IPv4 addresses are divided into 5 classes (A, B, C, D, E). Each class has a range of IP addresses. IP addresses from the first three classes are used for host addresses. Class D addresses are used for multicast, while class E addresses are used for experimental purposes as presented in Table 3.

*Table 1: Classes of IP*

Class	Address Range	IP Addresses Per Network	Subnet Mask
<b>Class A</b>	0.0.0.0 – 127.255.255.255	16,777,216	8
<b>Class B</b>	128.1.0.1 – 191.255.255.255	65,536	16
<b>Class C</b>	192.0.1.1 – 223.255.255.255	256	24
<b>Class D</b>	224.0.0.0 – 239.255.255.255		Reserved for multicast groups
<b>Class E</b>	240.0.0.0 – 255.255.255.255		Reserved for future use, research, and experimental purposes

Among these IP addresses, some are reserved for special purposes, while other are used for public and private networks. We will learn about them later.

## Subnetting / Classless Inter Domain Routing (CIDR)

An IP address is made up of the network part and the host part. The class of the IP address determines the network part and the host part. The function of the subnet mask is to split the IP address into the network part and the host part.



*When assigning IP Addresses, the network part does not change. For instance, the Class A network 14.0.0.0, the 14 which is the network part does not change when assigning IP addresses. The addresses will start with 14.0.0.1, 14.0.0.67, 14.0.3.4...14.255.255.255. Only the network part does not change.*



*List 5 possible IP addresses from these networks*

1. 175.100.0.0/16
2. 194.14.1.0/24

- **Class A** - first 8 bits is the network part; the remaining 24 bits is the network part. E.g., 10.0.0.0. The network part does not change. Also, class A networks have a total of 16,777,216 IP addresses per network. For instance, the Class A network 13.0.0.0/8 (/8 is the CIDR notation), has a total IP address of 16,777,216. Can you list them? 13.0.0.1, 13.0.0.255, 13.0.1.0, 13.0.1.255, and so forth

Class A Networks	Properties
Number of Networks	128 ( $2^7$ )
Total addresses per network	16,777,216 ( $2^{24}$ )
Total addresses for all networks	2,147,483,648 ( $2^{31}$ ) i.e., $2^7 \times 2^{24}$
Size of network bit	8
Size of host bit	24



Which of these networks are Class A networks? (Multiple choice allowed)

- A. 112.67.83.100
- B. 133.56.34.12
- C. 156.123.244.23
- D. 12.54.23.01

- **Class B** - first 16 bits is the network part; the remaining 16 bits is the network part. E.g., 172.169.0.0. Using a CIDR notation of /16, a Class B network has a maximum of 65,536, which is  $2^{16}$ . The total addresses for all Class B network are 1,073,741,824.

Class B Networks	Properties
Number of Networks	16384 ( $2^{14}$ )
Total addresses per network	65,536 ( $2^{16}$ )
Total addresses for all networks	1,073,741,824 ( $2^{30}$ ) i.e., $2^{14} \times 2^{16}$
Size of network bit	16
Size of host bit	16

- **Class C** - first 24 bits is the network part; the remaining 8 bits is the network part. E.g., 192.168.1.0

Class C Networks	Properties
Number of Networks	2,097,152 ( $2^{21}$ )
Total addresses per network	256 ( $2^8$ )
Total addresses for all networks	536,870,912 ( $2^{29}$ ) i.e., $2^{21} \times 2^8$
Size of network bit	24
Size of host bit	8

*Note* 192.168.0.0 is a class C address. The first 24 bits is the network part. The IP addresses in this network will count from 192.168.0.0, 192.168.0.1, 192.168.0.2...192.168.0.254, 192.168.0.255

A total of 256 addresses is in this network.

### 5.1.5 Special IP Addresses

- 0.0.0.0 - used for wildcard.
- 127.0.0.1 - loopback addresses
- Multicast addresses - 224.0.0.0 – 239.255.255.255

Source: <https://www.ibm.com/docs/vi/zos/2.3.0?topic=considerations-special-ip-addresses>



### 5.1.6 Private and Public IP Addresses

Private IP addresses are used in private networks. They are not routable through the internet. If these addresses want to communicate with the public networks, the router will block any attempt because they are not public addresses. We will focus on private IP addresses that used in a Local Area Network (LAN).

Three address blocks (see Table 4), are reserved for communication with a LAN, namely 10.0.0.0/8, 172.16.0.0/16 and 192.168.0.0/24

*Table 2: IP Ranges*

Address Block	Address Range	Numb of Addresses	Purpose
10.0.0.0/8	10.0.0.0 – 10.255.255.255	16,777,216	Used for local communications with a private network
172.16.0.0/16	172.16.0.0 – 172.31.255.255	65,536	Used for local communications with a private network
192.168.0.0/24	192.168.0.0 – 192.168.255.255	256	Used for local communications with a private network



*If two private networks want to communicate through the public network (internet), communications will be through an IP tunnel called a Virtual Private Network (VPN).*

### Public address

These are IP addresses assigned by a router for a host computer or device to communicate with the internet.



*If you are connected to the internet, visit [www.whatismyipaddress.com](http://www.whatismyipaddress.com) to find your public IP address.*

### 5.1.7 Static and Dynamic IP Addresses

An IP address can be static (does not change when the host disconnects from a network) or dynamic (changes whenever a host disconnects and reconnects to a network).

**Static address** is typed manually into your computer when you connect to a network using a LAN cable like UTP, STP, and Coaxial Cable. **Dynamic addressing** is managed by the router which uses a protocol called Dynamic Host Configuration Protocol (DHCP) for dynamic IP address allocation.

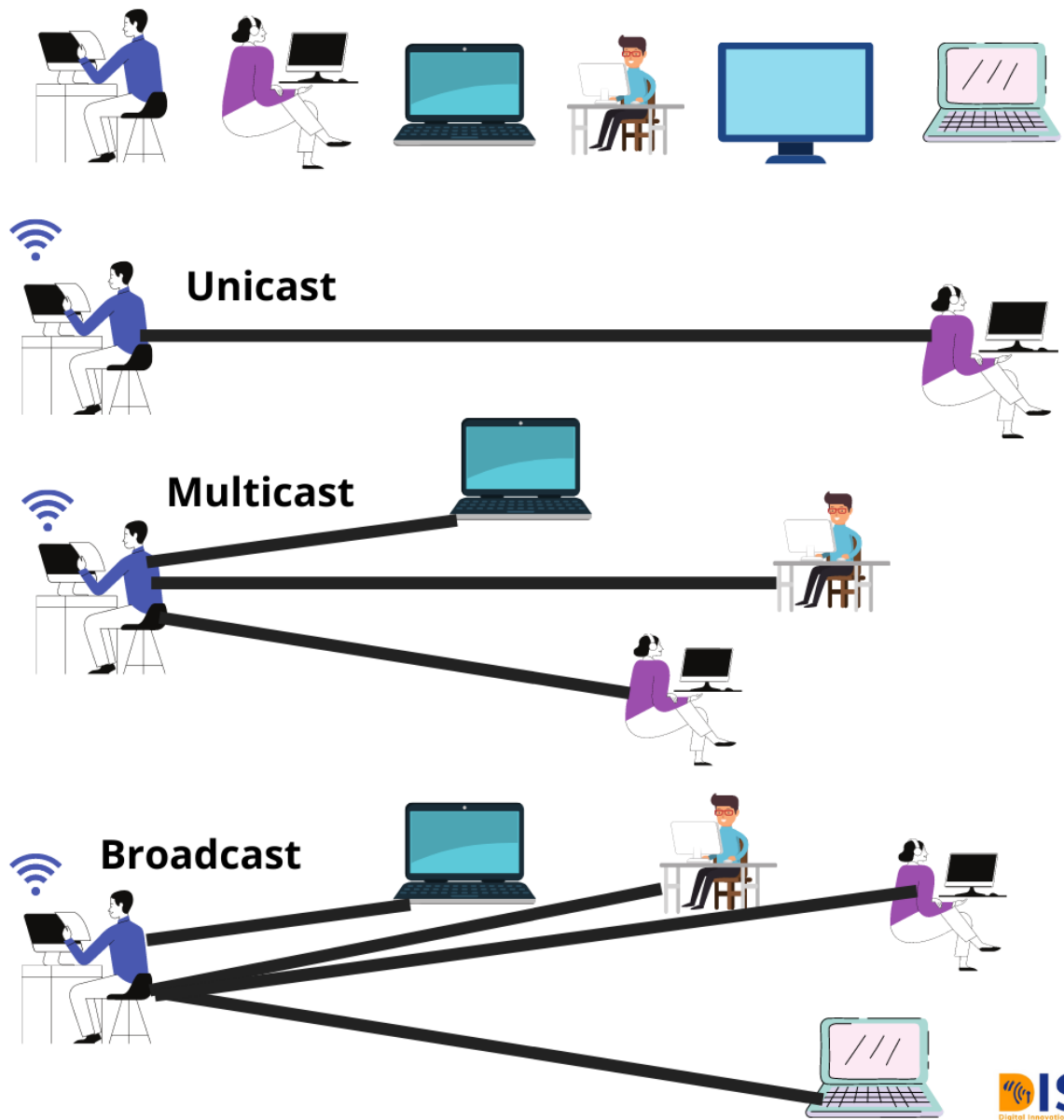
### 5.1.8 Network Address Translation

Allows private IP addresses to communicate with the internet. A single IP address can be used by a single or group of computers to access the internet. The router acts as an agent between the local network (private network) and the internet (public network).

## 6.2 Types of IP Addresses

There are three types of IP addresses, they are unicast addresses, multicast addresses and broadcast addresses.

1. **Unicast** – these IP addresses are used for one-to-one communication. They are the IP addresses assigned to hosts i.e., devices and computers connected to a computer network. An example of unicast IP addresses is 192.168.1.16. The first IP address in a range of address is always reserved for the router. For example, in the network 192.168.1.0/24, the first assignable address 192.168.1.1 is reserved for the router.
2. **Multicast** – multicast IP addresses are used for one-to-many communication. The messages are sent to some devices and computers in the network, not all devices in the network. Unicast sends from one computer to another computer. IP addresses from 224.0.0.0 – 239.255.255.255 are reserved for multicast communication in a network.
3. **Broadcast** – broadcast addresses are used to send messages to all devices in a network. Unlike unicast and multicast that send to one and many respectively, broadcast sends to all. The last IP addresses in a network are reserved for broadcast messaging. For instance, the network 10.0.0.0/8 has a total of 16,777,216 IP addresses. The last IP address 10.255.255.255 is reserved for broadcast. Another network 192.170.5.0/24 has a total of 256 IP addresses, the last IP address 192.170.5.255 is reserved for broadcast.



*Figure 3: Communication forms*

The Figure in 33, illustrates in detail the forms of communication with various IP addresses.

## **6.2 IPv6**

IPv6 was created to replace the commonly used IPv4 that is running out of addresses. It is made up of 128 bits divided into eight 16 bits blocks. Each block is usually represented in hexadecimal (base 16) and separated by a colon ':'

An IPV6 looks like this 2001:0000:3238: DFE1:63:0000:0000: FEFB

## **6.3 Network Topology**

Network topology is defined as the arrangement of computers in a network. It shows how computers, nodes, links, and network devices are connected to each other in a network. The topology also informs a User where a device or computer is to be located on a network. A good understanding of network topology will help in managing the resources available for the setting up of the network.

As a network administrator in a network, each arrangement has its advantages and disadvantages. The topology used in a network will determine how the network will be effectively managed, (for example troubleshooting a network can be made easier by its topology), and the resources required to setup the network.

A network topology can be physical or logical. Physical topology refers to the real connections that can be seen. For e.g., the actual physical location of routers, switches, computers, cabling, are seen in a physical topology.

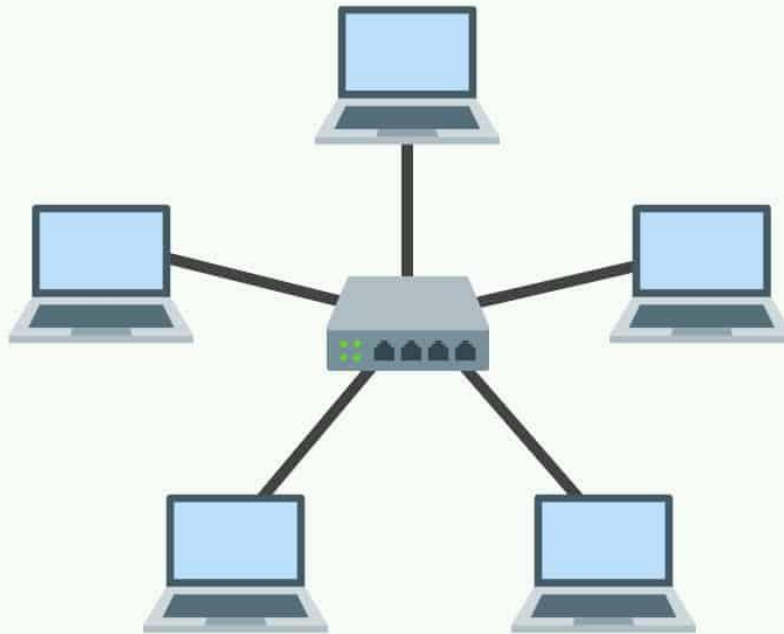
A logical topology gives a high-level view of how a network is arranged. It gives an overview of physical resources.

### 6.3.1 Types of Network Topology

The network topology to be chosen should be determined by the size of your network.

#### Star Topology

In this topology, every point in the network is connected to a single node/device or central hub. The central hub can be a router, switch, coaxial cable, fibre optics or twisted pair cable. The central station manages data transmission and directs traffic in the network (as shown in Figure 34).



*Figure 4: Star Topology. Credit - comparitech.com*

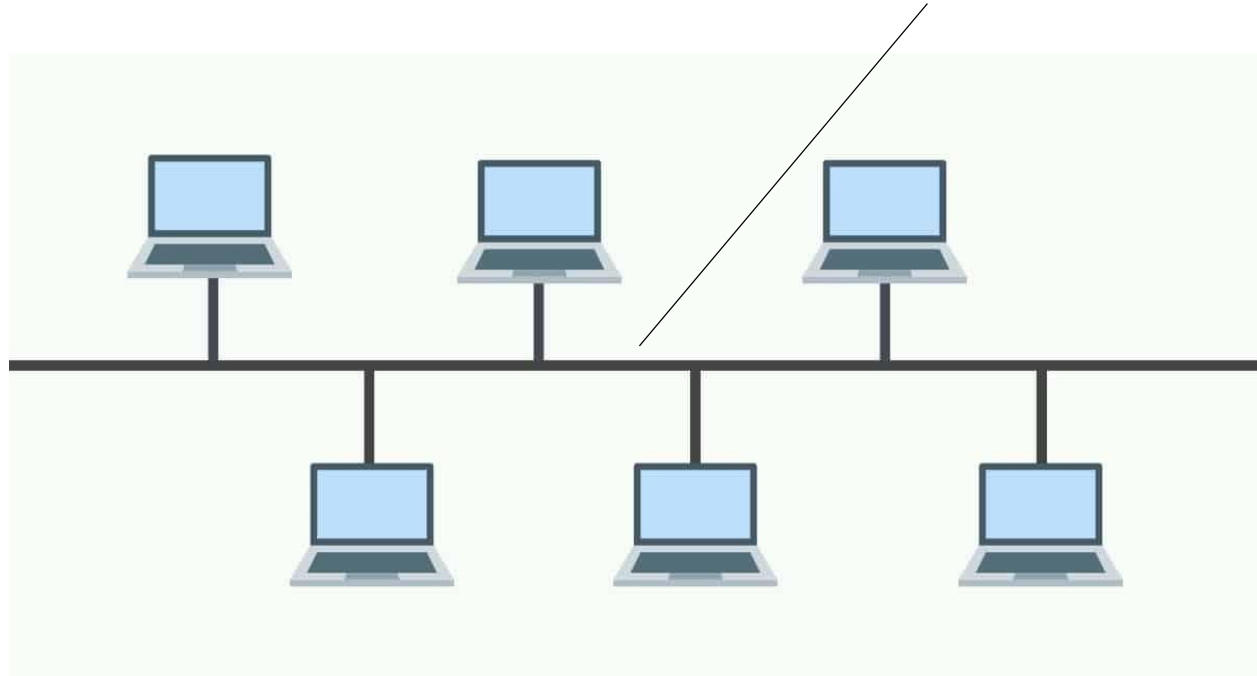
### **Advantages of Star Topology**

1. The network is easy to manage from a single point. It is suitable for smaller networks.
2. Devices, computers, and nodes can be removed without affecting the entire network.
3. It is easy to troubleshoot and fix any issue.
4. Star topology does not require complex cabling in a physical network. All you need is to connect the computer to the switch or hub

### **Disadvantages of Star Topology**

1. The entire network collapses if the central station is down.
2. The central station can limit the performance of the network. When the central station is not operating at an Optimal level, network performance collapses.

## Bus Topology



*Figure 5: Line or Bus. Credit – tutsmaster.org*

Also called line topology where all the hosts in the network are connected to a single line or bus. The line/bus is responsible for data flow with little cost implication as compared to the Star topology (Figure 32).

### Advantages of Bus Topology

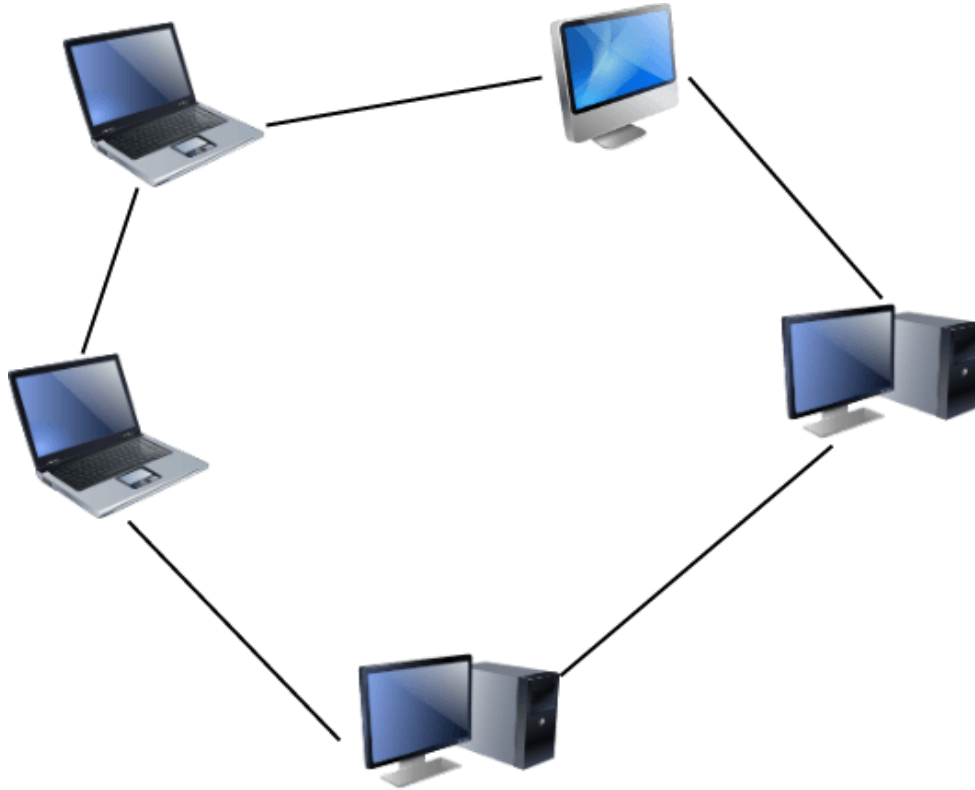
1. This topology is suitable where minimal network management is required.
2. It is easy to add new devices to this topology.

### Disadvantages of Bus Topology

1. The whole network goes down if the single line or bus collapses.
2. This topology is not ideal for networks with huge amount of traffic.
3. Data cannot be sent in opposite directions, i.e., The network is half duplex.



## Ring Topology



*Figure 6: Ring Topology. Credit – kenCorner.com*

In this topology, all the computers, devices and nodes in the network are arranged to form a ring. Every device connected to the network is important. Therefore, if any of them goes down, the entire network goes down. Also, data moves in one direction, because only one station (node) can send data per time. Today, ring topology is rarely used (Figure 33).

### Advantages of Ring Topology

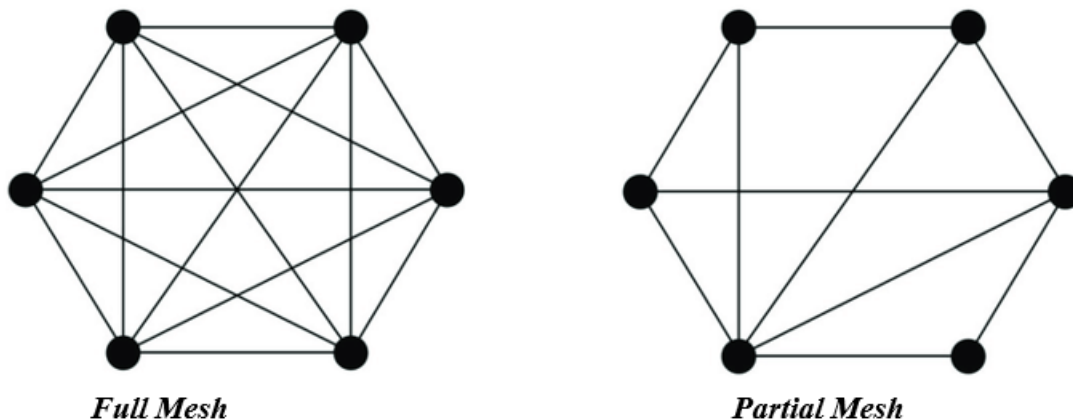
1. One computer can send packets per time. The packets travel round the ring nodes, till it gets to the destination.
2. Cheap to install and easy to maintain and troubleshoot.

### Disadvantages of Ring Topology

1. If one ring goes down, the entire network goes down with it.

### Mesh Topology

Mesh networks are where network nodes are interconnected to each other. All nodes in the network are connected to one another.



*Figure 37: Mesh Topology*

A mesh topology as illustrated in Figure 37, can be partial or full. Partial mesh has fewer nodes than full mesh. The mesh topology has many advantages compared to other types of network topologies.

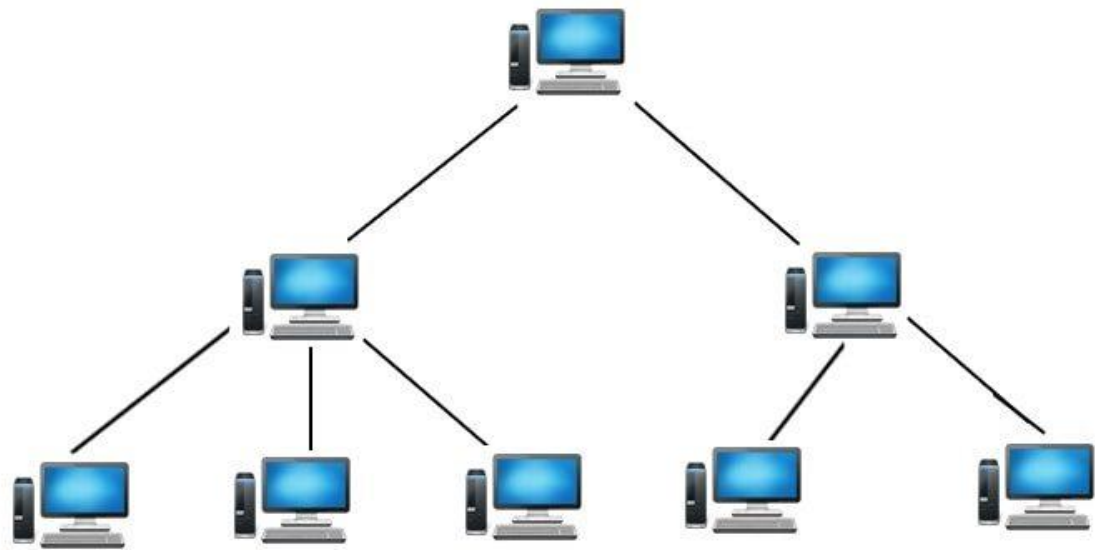
### Advantages of Mesh Topology

1. The network can hardly go down because there are different paths packets can be routed for successful data transmission.

### Disadvantages of Mesh Topology

1. It is expensive to setup and maintain.
2. A lot of cabling, configuration and labour are required for setup and administration.

## 6.1.5 Tree Topology



*Figure 7: Tree Topology. Credit – generalnote.com*

In this topology, every node in a network is linked to a central hub, also two nodes can only be connected to one mutual node. It creates a tree connection (parent-child relationship). This allows for scalability and easy network administration.