CN Notes

III unit II sem **Diksha Kumare**

Local Area Network :

A local area network (LAN) is a group of computers and peripheral devices that share a common communications line or wireless link to a server within a distinct geographic area. A local area network may serve as few as two or three users in a home office or thousands of users in a corporation's central office.

Ethernet : Ethernet is a type of communication protocol that was created at Xerox PARC in 1973 by Robert Metcalfe and others, which connects computers on a network over a wired connection. It is a widely used LAN protocol, which is also known as Alto Aloha Network. It connects computers within the local area network and wide area network. Numerous devices like printers and laptops can be connected by LAN and WAN within buildings, homes, and even small neighborhoods.

802.3 IEEE Standards :

IEEE 802.3 is a set of standards and protocols that define Ethernet-based networks. Ethernet technologies are primarily used in LANs, though they can also be used in MANs and even WANs. IEEE 802.3 defines the physical layer and the medium access control (MAC) sub-layer of the data link layer for wired Ethernet networks.

IEEE 802.3 Popular Versions

There are a number of versions of IEEE 802.3 protocol. The most popular ones are.

IEEE 802.3: This was the original standard given for 10BASE-5. It used a thick single coaxial cable into which a connection can be tapped by drilling into the cable to the core. Here, 10 is the maximum throughput, i.e. 10 Mbps, BASE denoted use of baseband transmission, and 5 refers to the maximum segment length of 500m.

IEEE 802.3a: This gave the standard for thin coax (10BASE-2), which is a thinner variety where the segments of coaxial cables are connected by BNC connectors. The 2 refers to the maximum segment length of about 200m (185m to be precise).

IEEE 802.3i: This gave the standard for twisted pair (10BASE-T) that uses unshielded twisted pair (UTP) copper wires as physical layer medium. The further variations were given by IEEE 802.3u for 100BASE-TX, 100BASE-T4 and 100BASE-FX.

IEEE 802.3i: This gave the standard for Ethernet over Fiber (10BASE-F) that uses fiber optic cables as medium of transmission.

Frame Format of IEEE 802.3

The main fields of a frame of classic Ethernet are -

Preamble: It is a 7 byte starting field that provides alert and timing pulse for transmission.

Start of Frame Delimiter: It is a 1 byte field that contains an alternating pattern of ones and zeros ending with two ones.

Destination Address: It is a 6 byte field containing the physical address of destination stations.

Source Address: It is a 6 byte field containing the physical address of the sending station.

Length: It is a 7 bytes field that stores the number of bytes in the data field.

Data: This is a variable sized field that carries the data from the upper layers. The maximum size of the data field is 1500 bytes.

Padding: This is added to the data to bring its length to the minimum requirement of 46 bytes.

CRC: CRC stands for cyclic redundancy check. It contains the error detection information.

Token Ring Network (IEEE Standard 802.5)

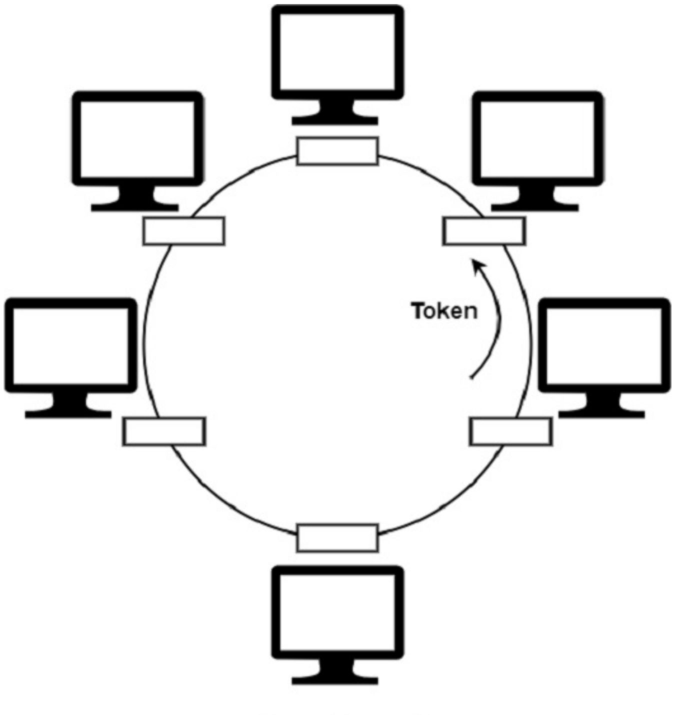
In a token ring, a special bit pattern, known as a token, circulates around the ring when all the stations are idle. Token Ring is formed by the nodes connected in ring format, as shown in the diagram below.

The principle used in the token ring network is that a token is circulating in the ring, and whichever node grabs that token will have the right to transmit the data.

Whenever a station wants to transmit a frame, it inverts a single bit of the 3-byte token, which instantaneously changes it into a normal data packet. As there is only one token, there can be only one transmission at a time.

Since the token rotates in the ring, it is guaranteed that every node gets the token within some specified time. So there is an upper bound on the time of waiting to grab the token so that starvation is avoided. There is also an upper limit of 250 on the number of nodes in the network.

The ring network is depicted in the figure given below −



Ring Network

Modes of Operation

There are various modes of operations which are as follows −

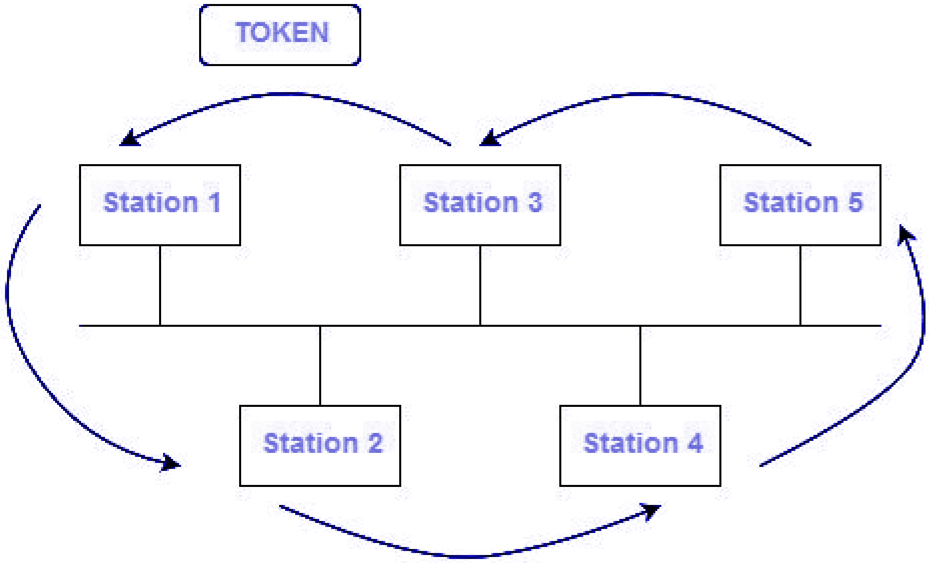
Listen Mode − In the listen mode, the incoming bits are simply transmitted to the output line with no further action taken.

Talk or Transmit Node − The ring interface is set to the talk or transmit node when the station connected to the ring interface has acquired a token. The direct input to output connection through the single bit buffer is disconnected.

By-pass Mode − This mode reaches when the node is down. Any data is just bypassed. There is no one-bit delay in this mode.

Token Bus (IEEE 802.4) : It is a popular standard for token passing LANs. In a token bus LAN, the physical media is a bus or a tree, and a logical ring is created using a coaxial cable. The token is passed from one user to another in a sequence (clockwise or anticlockwise). Each station knows the address of the station to its “left” and “right” as per the sequence in the logical ring. A station can only transmit data when it has the token. The working of a token bus is somewhat similar to Token Ring.

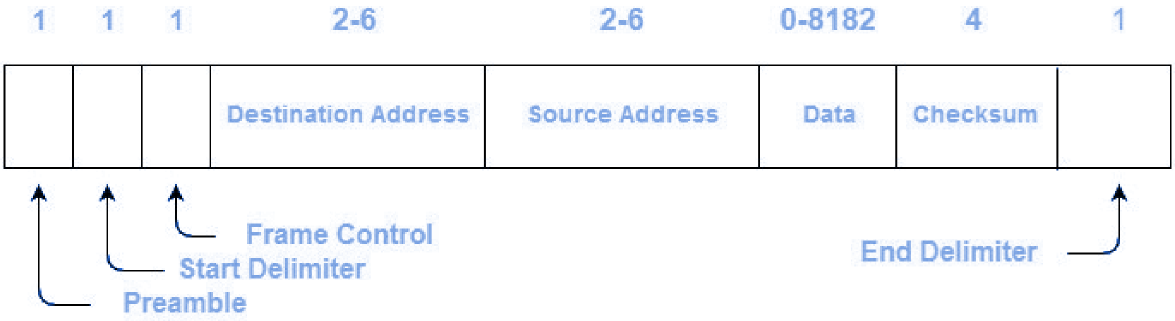
The Token Bus (IEEE 802.4) is a standard for deploying token rings in LANs over a virtual ring. The physical medium uses coaxial cables and has a bus or tree architecture. The nodes/stations form a virtual ring, and the token is transmitted from one node to the next in a sequence along the virtual ring. Each node knows the address of the station before it and the station after it. When a station has the token, it can only broadcast data. The token bus works in a similar way as the Token Ring.



The above diagram shows a logical ring formed in a bus-based token-passing LAN. The logical ring is shown with the arrows.

Frame Format:

The various fields of the frame format are:



1. **Preamble –** It is used for bit synchronization. It is a 1-byte field.
2. **Start Delimiter –** These bits mark the beginning of the frame. It is a 1-byte field.
3. **Frame Control –** This field specifies the type of frame – data frame and control frames. It is a 1-byte field.
4. **Destination Address –** This field contains the destination address. It is a 2 to 6 byte field.
5. **Source Address –** This field contains the source address. It is a 2 to 6 byte field.
6. **Data –** If 2-byte addresses are used then the field may be up to 8182 bytes and 8174 bytes in the case of 6-byte addresses.
7. **Checksum –** This field contains the checksum bits which are used to detect errors in the transmitted data. It is a 4 bytes field.
8. **End Delimiter –** This field marks the end of a frame. It is a 1-byte field.

FDDI Protocol : Fiber Distributed Data Interface (FDDI) is a set of ANSI and ISO standards for transmission of data in local area network (LAN) over fiber optic cables. It is applicable in large LANs that can extend up to 200 kilometers in diameter.

Features : FDDI uses optical fiber as its physical medium.
It operates in the physical and medium access control (MAC layer) of the Open Systems Interconnection (OSI) network model.

It provides a high data rate of 100 Mbps and can support thousands of users.

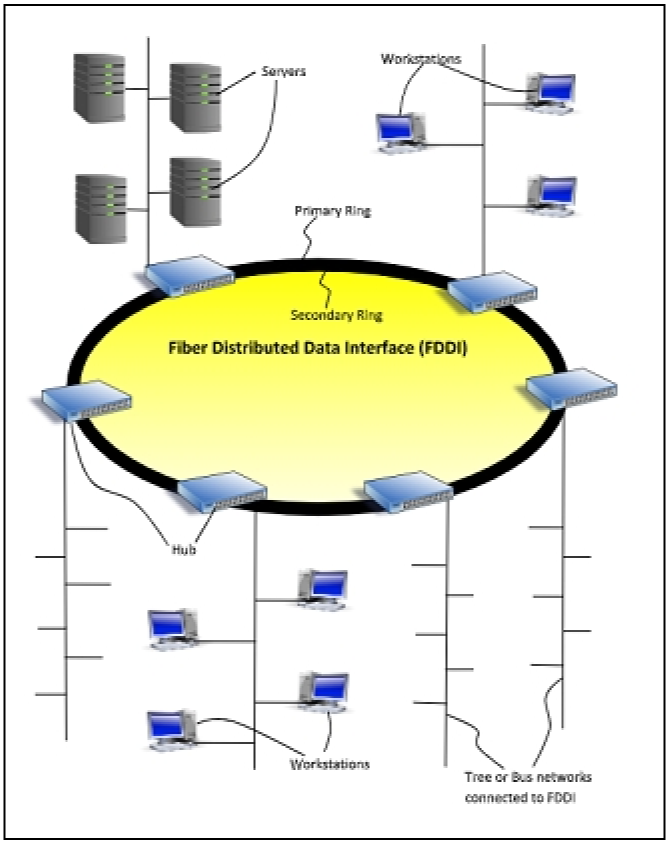
It is used in LANs up to 200 kilometers for long distance voice and multimedia communication.

It uses a ring based token passing mechanism and is derived from IEEE 802.4 token bus standard.

It contains two token rings, a primary ring for data and token transmission and a secondary ring that provides backup if the primary ring fails.

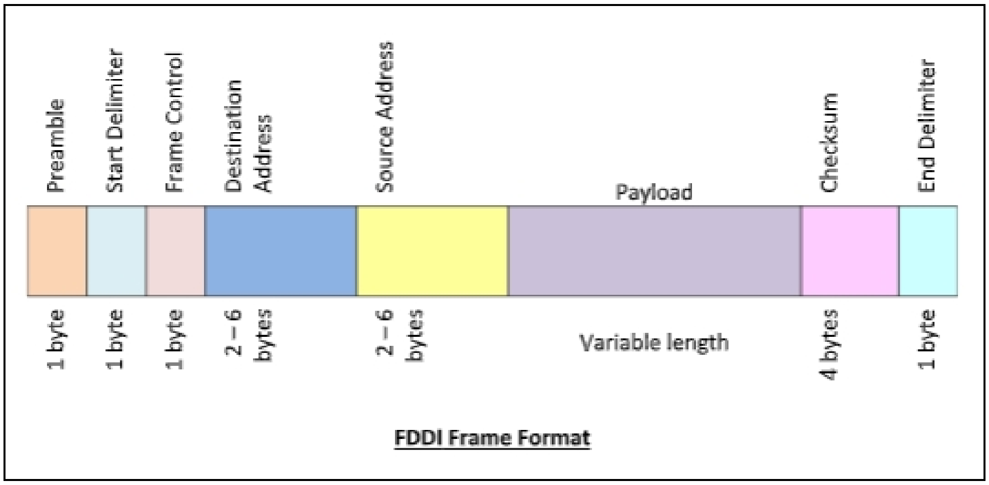
FDDI technology can also be used as a backbone for a wide area network (WAN).

The following diagram shows FDDI −


Servers
Workstations
Primary Ring
Secondary Ring
Fiber Distributed Data Interface (FDDI)
Hub
Workstations
Tree or Bus networks connected to FDDI

Frame Format

The frame format of FDDI is similar to that of token bus as shown in the following diagram −



Preamble	Start Delimiter	Frame Control	Destination Address	Source Address	Payload	Checksum	End Delimiter
1 byte	1 byte	1 byte	2 – 6 bytes	2 – 6 bytes	Variable length	4 bytes	1 byte

FDDI Frame Format

The fields of an FDDI frame are −

Preamble: 1 byte for synchronization.

Start Delimiter: 1 byte that marks the beginning of the frame.

Frame Control: 1 byte that specifies whether this is a data frame or control frame.

Destination Address: 2-6 bytes that specifies address of destination station.

Source Address: 2-6 bytes that specifies address of source station.

Payload: A variable length field that carries the data from the network layer.

Checksum: 4 bytes frame check sequence for error detection.

End Delimiter: 1 byte that marks the end of the frame.

DQDB Protocol : IEEE 802.6, or Distributed Queue Dual Bus (DQDB), is a metropolitan area network (MAN) technology for LANs developed by the Institute for Electrical and Electronic Engineers' Committee for Computer Communications Standards. It is designed for use in metropolitan areas with wide geographical coverage, such as cities, campuses, and other places where the users are linked together over distances up to 10 kilometers apart. The fundamental idea behind DQDB is to build numerous virtual buses that can be utilized for two endpoints on a network to communicate in both directions. Each bus has its own unique address for identification and allows for reservation-based access for data transmission across different nodes in the network.

Features, specifications, applications and aspects of IEEE 802.6 (DQDB) :

IEEE 802.6 (Distributed Queue Dual Bus) is a standard for metropolitan area networks (MANs) that was developed by the IEEE. This standard provides a high-speed, reliable, and efficient communication system for MANs. In this article, the features, specifications, applications, and aspects of IEEE 802.6 (DQDB) will be discussed.

Features of IEEE 802.6 (DQDB)

IEEE 802.6 (DQDB) has several features that make it an ideal communication system for MANs. These features include −

Distributed Queuing − IEEE 802.6 (DQDB) uses a distributed queuing algorithm that ensures fair access to the network by all users. This algorithm also provides a low latency, which is essential for real-time applications.

Dual Bus Architecture − IEEE 802.6 (DQDB) uses a dual-bus architecture that provides redundancy and fault tolerance. If one bus fails, the other bus takes over, ensuring continuous communication.

Token Passing Mechanism − IEEE 802.6 (DQDB) uses a token passing mechanism to control access to the network. This mechanism ensures that only one station can transmit data at a time, preventing collisions and ensuring efficient use of the network.

Specifications of IEEE 802.6 (DQDB)

Specification	Description

Data Rate	IEEE 802.6 (DQDB) supports a data rate of up to 155 Mbps, which is sufficient for most applications.
Distance	IEEE 802.6 (DQDB) supports a maximum distance of 25 km, making it suitable for MANs.
Frame Size	IEEE 802.6 (DQDB) supports a frame size of up to 4480 bytes, which is larger than the frame size supported by other LAN technologies.
Topology	IEEE 802.6 (DQDB) uses a dual ring topology with two counter-rotating rings, providing redundancy and fault tolerance.
Access Method	IEEE 802.6 (DQDB) uses a distributed queue dual bus (DQDB) access method, which supports both connection-oriented and connectionless data transfers.
QoS Support	IEEE 802.6 (DQDB) provides support for quality of service (QoS) mechanisms, including bandwidth allocation and priority-based packet scheduling.
Addressing	IEEE 802.6 (DQDB) uses a 48-bit MAC address format to uniquely identify devices on the network.

Medium	IEEE 802.6 (DQDB) uses fiber-optic or twisted-pair cables as the transmission medium, providing high bandwidth and low latency.

Applications of IEEE 802.6 (DQDB)

IEEE 802.6 (DQDB) has several applications in MANs. These applications include −

Video Conferencing − IEEE 802.6 (DQDB) provides a high-speed and reliable communication system that is ideal for video conferencing.

Real-Time Applications − IEEE 802.6 (DQDB) provides a low latency and efficient communication system that is essential for real-time applications such as online gaming and live streaming.

Data Transfer − IEEE 802.6 (DQDB) provides a high-speed communication system that is ideal for data transfer applications such as file sharing and data backup.

Aspects of IEEE 802.6 (DQDB)

IEEE 802.6 (DQDB) has several aspects that make it an ideal communication system for MANs. These aspects include −

Scalability − IEEE 802.6 (DQDB) can be easily scaled up to accommodate a large number of users and devices.

Reliability − IEEE 802.6 (DQDB) provides a reliable communication system that is essential for critical applications.

Cost-Effective − IEEE 802.6 (DQDB) provides a cost-effective communication system that is suitable for small and medium-sized businesses.

IEEE 802.6 (DQDB) is a standard for metropolitan area networks that provides a high-speed, reliable, and efficient communication system. Its distributed queuing algorithm, dual-bus architecture, and token passing mechanism make it an ideal communication system for MANs. It supports a rate of data of up to 155 Mbps, a maximum distance of 25 km, and a frame size of up to 4480 bytes. Its applications include video conferencing, real-time applications, and data transfer. Its scalability, reliability, and cost-effectiveness make it a popular choice for small and medium-sized businesses. Overall, IEEE 802.6 (DQDB) is a powerful and versatile standard that has had a significant impact on the development of modern communication systems.

Advantages and Disadvantages of IEEE 802.6 (DQDB)

The main advantages of IEEE 802.6 are its scalability, reliability, speed, and cost effectiveness for metropolitan area networks with wide geographical coverage. The protocol is also efficient for multimedia applications such as video conferencing, interactive gaming, and high-speed digital data communication for office or business networks due to its fast transmission rates. Additionally, it can be implemented on existing LAN wiring which makes installation easy and costs less than conventional wireless systems.

IEEE 802.6 has some disadvantages as well. The protocol is not suitable for networks spanning longer distances or for larger networks due to its limited transmission range and bandwidth limitations for data transfer rates. In addition, the protocol does not support Quality of Service (QoS) for multimedia applications which may limit its effectiveness for some applications requiring high quality video or audio streaming.

Inter Networking : Internetworking is a combination of 2 words, inter and networking which implies an association between totally different nodes or segments. This connection area unit is established through intercessor devices akin to routers or gateway. The first term for associate degree internetwork was catenet. This interconnection is often among or between public, private, commercial, industrial, or governmental networks. Thus, associate degree internetwork could be an assortment of individual networks, connected by intermediate networking devices, that function as one giant network. Internetworking refers to the trade, products, and procedures that meet the challenge of making and administering internet works.

To enable communication, every individual network node or phase is designed with a similar protocol or communication logic, that is Transfer Control Protocol (TCP) or Internet Protocol (IP). Once a network communicates with another network having constant communication procedures, it’s called Internetworking. Internetworking was designed to resolve the matter of delivering a packet of information through many links.

There is a minute difference between extending the network and Internetworking. Merely exploitation of either a switch or a hub to attach 2 local area networks is an extension of LAN whereas connecting them via the router is an associate degree example of Internetworking. Internetworking is enforced in Layer three (Network Layer) of the OSI-ISO model. The foremost notable example of internetworking is the Internet.

There is chiefly 3 units of Internetworking:

1. Extranet
2. Intranet
3. Internet

Intranets and extranets might or might not have connections to the net. If there is a connection to the net, the computer network or extranet area unit is usually shielded from being accessed from the net if it is not authorized. The net isn't thought-about to be a section of the computer network or extranet, though it should function as a portal for access to parts of the associate degree extranet.

Extranet – It's a network of the internetwork that's restricted in scope to one organization or entity however that additionally has restricted connections to the networks of one or a lot of different sometimes, however not essential. It's the very lowest level of Internetworking, usually enforced in an exceedingly personal area. Associate degree extranet may additionally be classified as a Man, WAN, or different form of network however it cannot encompass one local area network i.e. it should have a minimum of one reference to associate degree external network.

Intranet – This associate degree computer network could be a set of interconnected networks, which exploits the Internet Protocol and uses IP-based tools akin to web browsers and FTP tools, that are underneath the management of one body entity. That body entity closes the computer network to the remainder of the planet and permits solely specific users. Most typically, this network is the internal network of a corporation or different enterprise. An outsized computer network can usually have its own internet server to supply users with browsable data.

Internet – A selected Internetworking, consisting of a worldwide interconnection of governmental, academic, public, and personal networks based mostly upon the Advanced analysis comes Agency Network (ARPANET) developed by ARPA of the U.S. Department of Defense additionally home to the World Wide Web (WWW) and cited as the 'Internet' to differentiate from all different generic Internetworks. Participants within the web, or their service suppliers, use IP Addresses obtained from address registries that manage assignments.

Internetworking has evolved as an answer to a few key problems: isolated LANs, duplication of resources, and an absence of network management. Isolated LANs created transmission problems between totally different offices or departments. Duplication of resources meant that constant hardware and code had to be provided to every workplace or department, as did a separate support employee. This lack of network management meant that no centralized methodology of managing and troubleshooting networks existed.

One more form of the interconnection of networks usually happens among enterprises at the Link Layer of the networking model, i.e. at the hardware-centric layer below the amount of the TCP/IP logical interfaces. Such interconnection is accomplished through network bridges and network switches. This can be typically incorrectly termed internetworking, however, the ensuing system is just a bigger, single subnetwork, and no internetworking protocol, akin to web Protocol, is needed to traverse these devices.

However, one electronic network is also reborn into associate degree internetwork by dividing the network into phases and logically dividing the segment traffic with routers. The Internet Protocol is meant to supply an associate degree of unreliable packet service across the network. The design avoids intermediate network components maintaining any state of the network. Instead, this task is allotted to the endpoints of every communication session. To transfer information correctly, applications should utilize associate degree applicable Transport Layer protocol, akin to Transmission management Protocol (TCP), that provides a reliable stream. Some applications use a less complicated, connectionless transport protocol, User Datagram Protocol (UDP), for tasks that don't need reliable delivery of information or that need period of time service, akin to video streaming or voice chat.

Internetwork Addressing –

Internetwork addresses establish devices severally or as members of a bunch. Addressing schemes differ based on the protocol family and therefore the OSI layer. Three kinds of internetwork address area units are ordinarily used: data-link layer addresses, Media Access control (MAC) addresses, and network-layer addresses.

Data Link Layer addresses: A data-link layer address unambiguously identifies every physical network association of a network device. Data-link addresses typically are area units cited as physical or hardware addresses. Data-link addresses sometimes exist among a flat address area and have a pre-established and usually fastened relationship to a selected device. End systems usually have just one physical network association, and therefore have just one data-link address. Routers and different internetworking devices usually have multiple physical network connections and so eventually have multiple data-link addresses.

MAC Addresses: Media Access management (MAC) addresses encompass a set of data-link layer addresses. MAC addresses establish network entities in LANs that implement the IEEE MAC addresses of the data-link layer. MAC addresses different area units distinctively for every local area network interface. MAC addresses are forty-eight bits long and are expressed in the form of twelve hexadecimal digits. The primary half dozen hexadecimal digits, which are usually administered by the IEEE, establish the manufacturer or merchant and therefore comprise the Organizational Unique Identifier (OUI). The last half dozen positional notation digits comprise the interface serial variety or another price administered by the particular merchant. MAC addresses are typically area units referred to as burned-in addresses (BIAs) as a result of being burned into read-only memory(ROM) and are traced into random-access memory (RAM) once the interface card initializes.

Network-Layer Addresses: Network addresses sometimes exist among a gradable address area and typically area units referred to as virtual or logical addresses. The connection between a network address and a tool is logical and unfixed, it usually relies either on physical network characteristics or on groupings that don't have any physical basis. finish systems need one network-layer address for every network-layer protocol they support. Routers and different Internetworking devices need one network-layer address per physical network association for every network-layer protocol supported.

Layer 1 : connections- Repeater, Hub :

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 details 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.

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.

Layer 2 connections- Bridges, Switches :

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 bridges 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.

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.

Types of Switch

1. Unmanaged switches: These switches have a simple plug-and-play design and do not offer advanced configuration options. They are suitable for small networks or for use as an expansion to a larger network.
2. Managed switches: These switches offer advanced configuration options such as VLANs, QoS, and link aggregation. They are suitable for larger, more complex networks and allow for centralized management.
3. Smart switches: These switches have features similar to managed switches but are typically easier to set up and manage. They are suitable for small- to medium-sized networks.

Layer 2 switches: These switches operate at the Data Link layer of the OSI model and are responsible for forwarding data between devices on the same network segment.

Layer 3 switches: These switches operate at the Network layer of the OSI model and can route data between different network segments. They are more advanced than Layer 2 switches and are often used in larger, more complex networks.

PoE switches: These switches have Power over Ethernet capabilities, which allows them to supply power to network devices over the same cable that carries data.

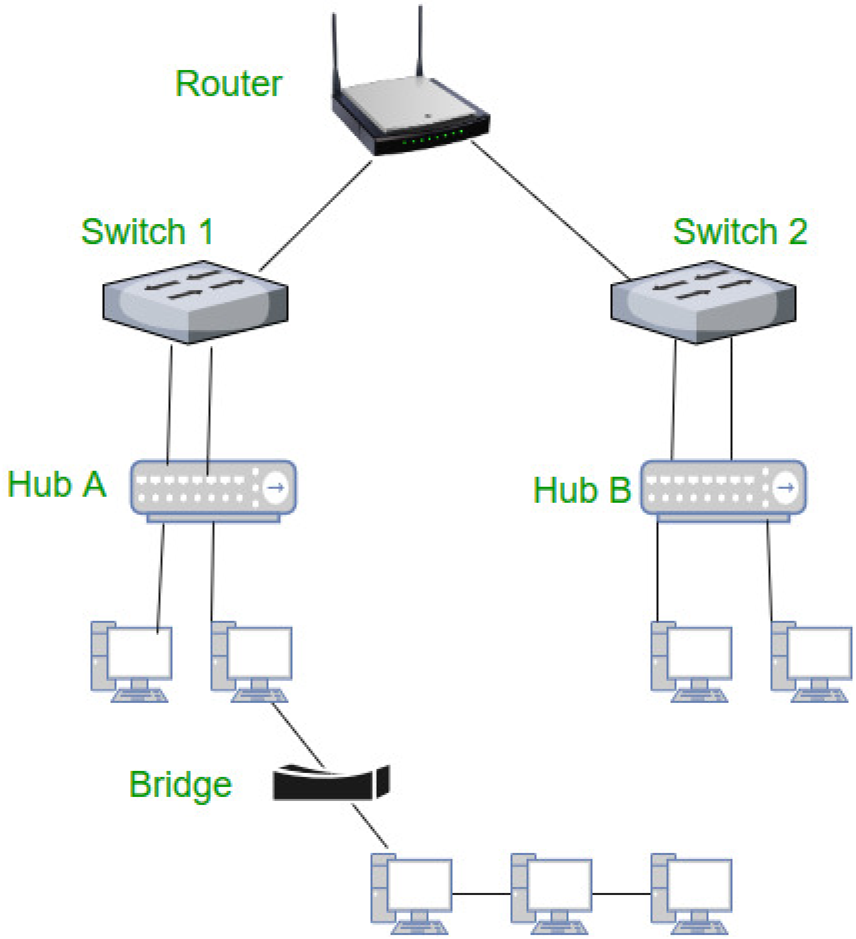
Gigabit switches: These switches support Gigabit Ethernet speeds, which are faster than traditional Ethernet speeds.

Rack-mounted switches: These switches are designed to be mounted in a server rack and are suitable for use in data centers or other large networks.

Desktop switches: These switches are designed for use on a desktop or in a small office environment and are typically smaller in size than rack-mounted switches.

Modular switches: These switches have modular design, which allows for easy expansion or customization. They are suitable for large networks and data centers.

Layer 3 connections- Routers, Gateways : 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.



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.