Data Communication

BCE 6th Semester

Er. Anuj Sherchan

Assistant Professor, Pokhara Engineering College

Unit 5: Overview of Data Communication Networking

- **Outline:**
- Network Types, Topology
- OSI Layers and Functions, TCP/IP Layers
- LAN Architecture, LLC/MAC and Routing
- IEEE Standards, Ethernet(CSMA/CD), Wide Area Networks: X.25, Frame Relay. ATM

Network Types

- A computer network is broadly classified into three types:
- Local Area Network (LAN),
- Metropolitan Area Network (MAN), and
- Wide Area Network (WAN).
- The different network types are distinguished from each other based on the following characteristics:
  - Size of the network
  - Transmission Technology
  - Networking Topology

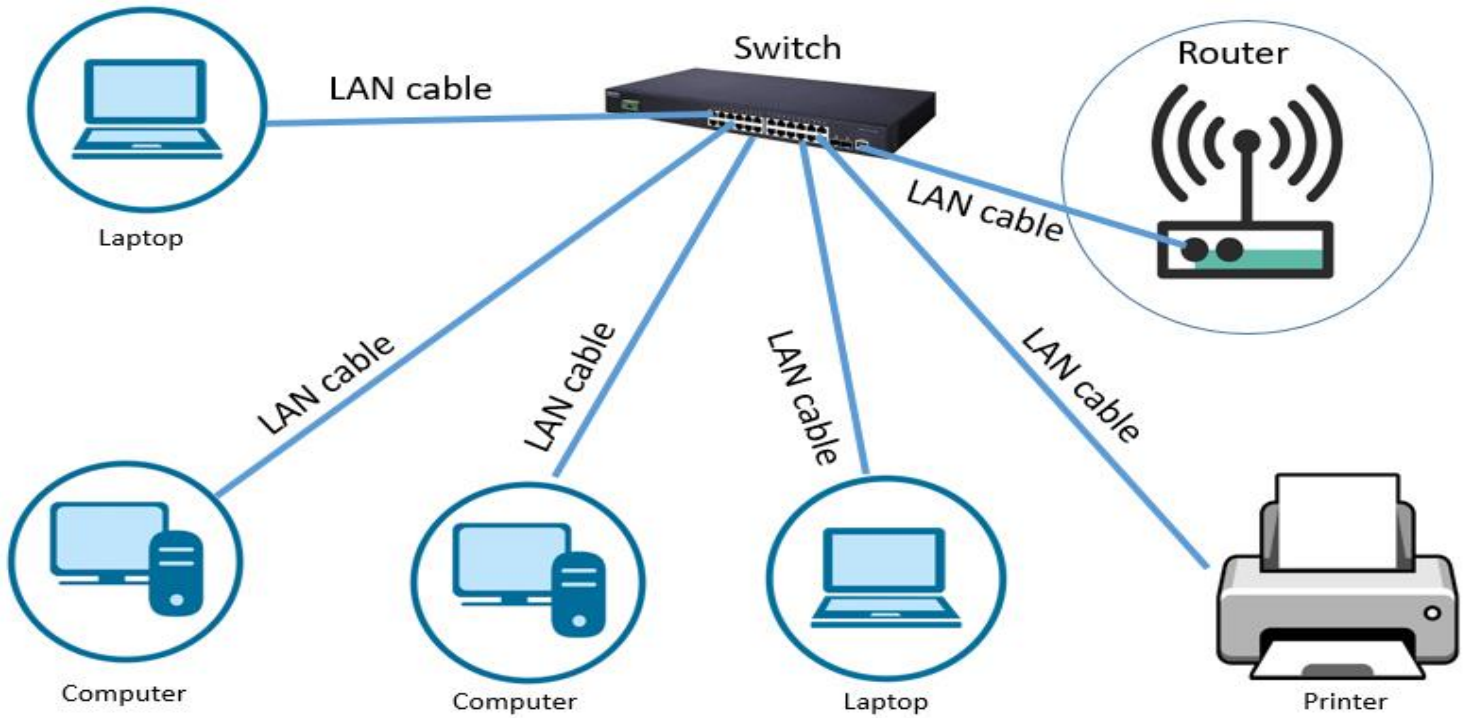
Network Types

- The size of the network refers to the area over which the network is spread.
- Transmission technology refers to the transmission media used to connect computers on the network and the transmission protocols used for connecting.
- Network topology refers to the arrangement of computers on the network or the shape of the network.
- **Local Area Network**
- LAN is a computer network widely used for local communication.
- LAN connects computers in a small area like a room, building, office or campus spread up to a few kilometers.
- They are privately owned networks, with the purpose to share resources and exchanging information.

Network Types

- The computers in a LAN are generally connected using cables.
- LAN is different from other types of the network since they share the network.
- The different computers connected to a LAN take turns sending data packets over the cables connecting them.
- This requires coordination of the use of the network.
- Some of the transmission protocols used in LAN are Ethernet and Token bus.
- Star, Bus, and Ring are some of the common LAN networking topologies.
- LAN runs at a speed of 10 Mbps to 100 Mbps and has low delays.
- A LAN based on Wi-Fi wireless network technology is called a Wireless Local Area Network (WLAN).

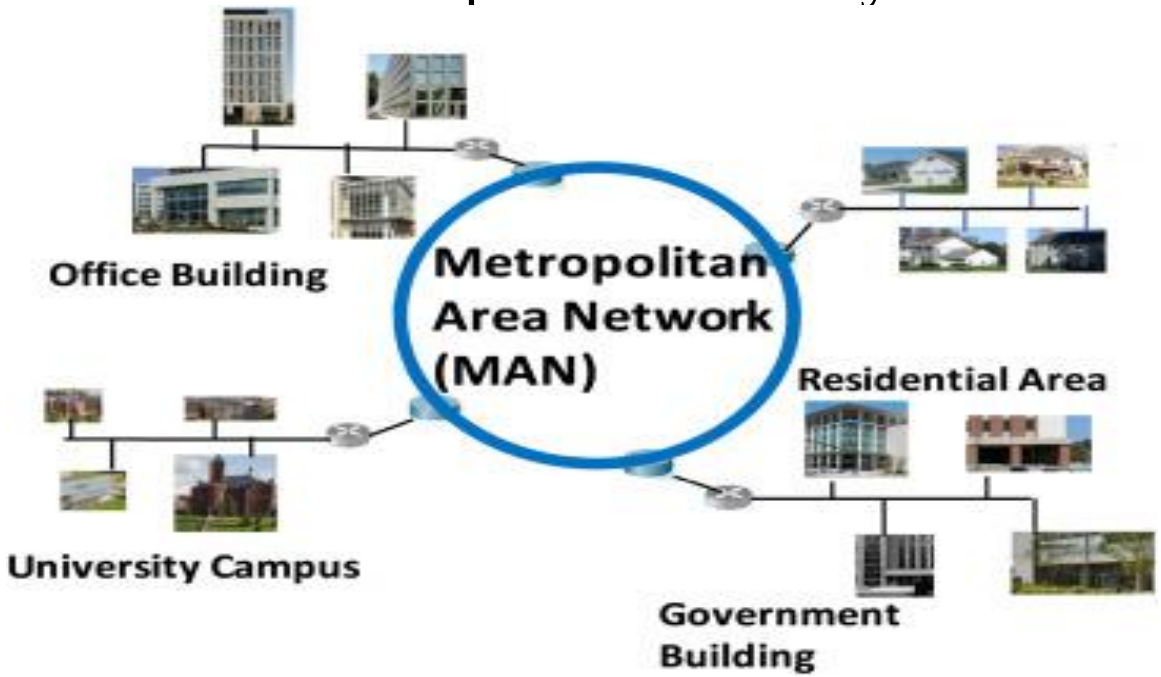
Network Types



Local Area Network

Network Types

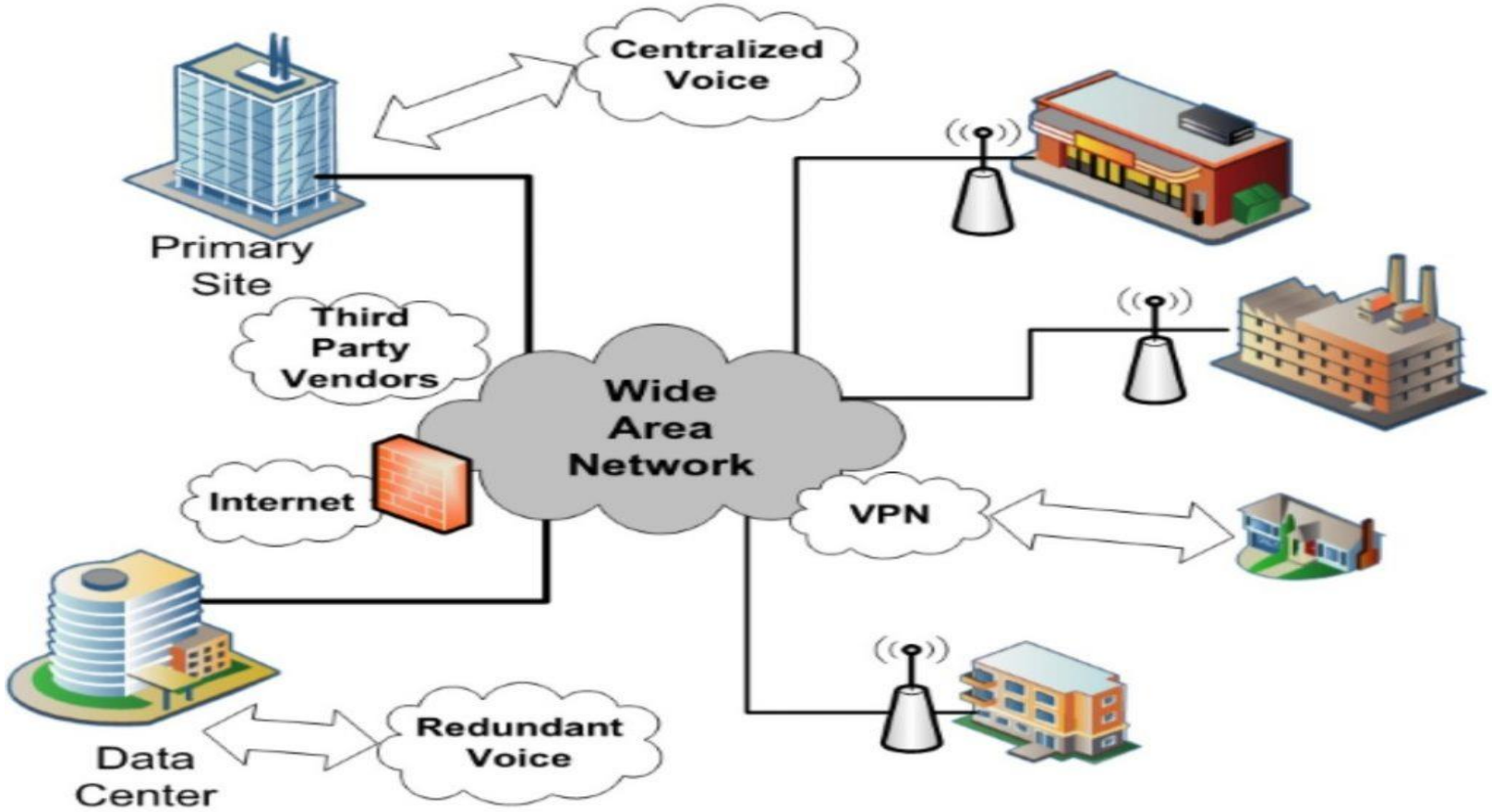
- **Metropolitan Area Network**
- MAN is a computer network spread over a city.
- Cable television network is an example of MAN.
- The computers in a MAN are connected using coaxial cables or fiber optic cables.
- MAN also connects several LANs spread over a city.
-



Network Types

- **Wide Area Network**
- WAN is a network that connects computers over long distances like cities, countries, continents, or worldwide.
- WAN uses public, leased, or private communication links to spread over long distances.
- WAN uses telephone lines, satellite links, and radio links to connect.
- The need to be able to connect any number of computers at any number of sites, results in WAN technologies being different from the LAN technologies.
- WAN network must be able to grow itself.
- Internet is a common example of WAN.

Network Types



Topology

- There are different types of network topologies that are used in a network.
- The network topologies are the structure or the layout of the different devices and computers connected to the network.
- The topologies commonly used in LAN are
- Bus topology,
- Star topology,
- Mesh Topology and
- Ring topology.

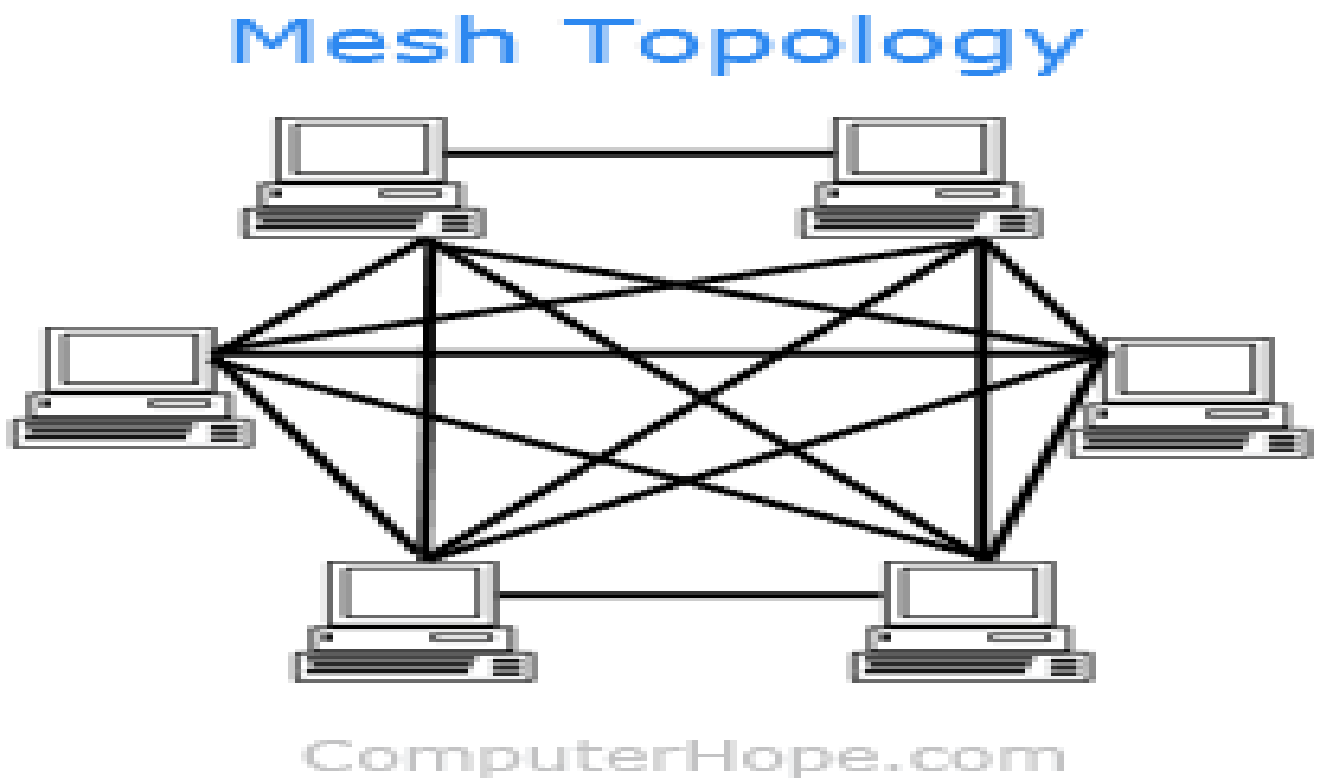
Topology

- **Mesh Topology**
- Mesh topology is a type of networking where all nodes cooperate to distribute data amongst each other.
- In a mesh topology, each device is connected to every other device on the network through a dedicated
point-to-point link.
- When we say dedicated it means that the link only carries data for the two connected devices only.
- **Advantages of Mesh topology**
- No data traffic issues as there is a dedicated link between two devices which means the link is only available for those two devices.

Topology

- Mesh topology is reliable and robust as the failure of one link doesn’t affect other links and the communication between other devices on the network.
- Mesh topology is secure because there is a point-to-point link thus unauthorized access is not possible.
- Fault detection is easy.
- **Disadvantages of Mesh topology**
- Amount of wires required to connect each system is tedious and a headache.
- Since each device needs to be connected with other devices, the number of I/O ports required must be huge.
- Scalability issues because a device cannot be connected with a large number of devices with a dedicated point-to-point link.

Topology



Topology

- **Star Topology**
- In star topology each device in the network is connected to a central device called a hub.
- Unlike Mesh topology, star topology doesn’t allow direct communication between devices, a device must have to communicate through the hub.
- If one device wants to send data to another device, it has to first send the data to the hub and then the hub transmits that data to the designated device.
- **Advantages of Star topology**
- Less expensive because each device only needs one I/O port and needs to be connected with a hub with one link.

Topology

- Easier to install
- Less amount of cables required because each device needs to be connected with the hub only.
- Robust, if one link fails, other links will work just fine.
- Easy fault detection because the link can be easily identified.
- **Disadvantages of Star topology**
- If the hub goes down everything goes down, none of the devices can work without the hub.
- Hub requires more resources and regular maintenance because it is the central system of star topology.

Topology

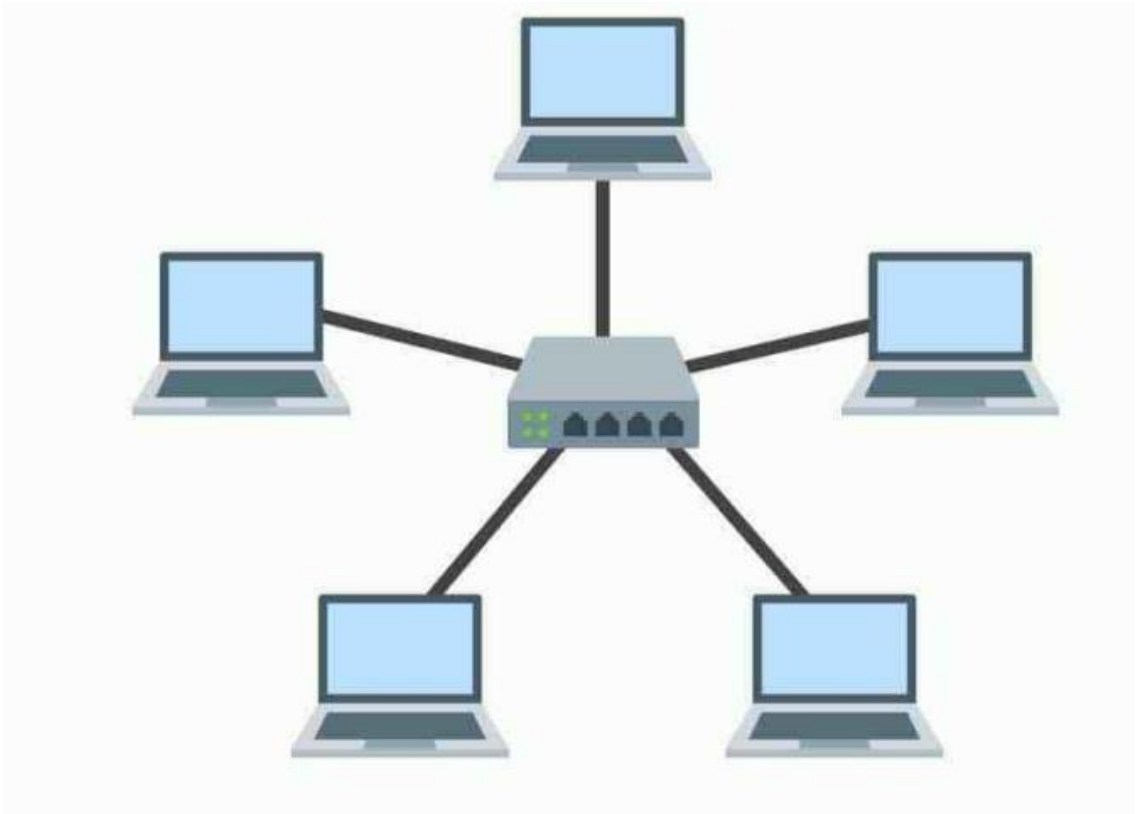


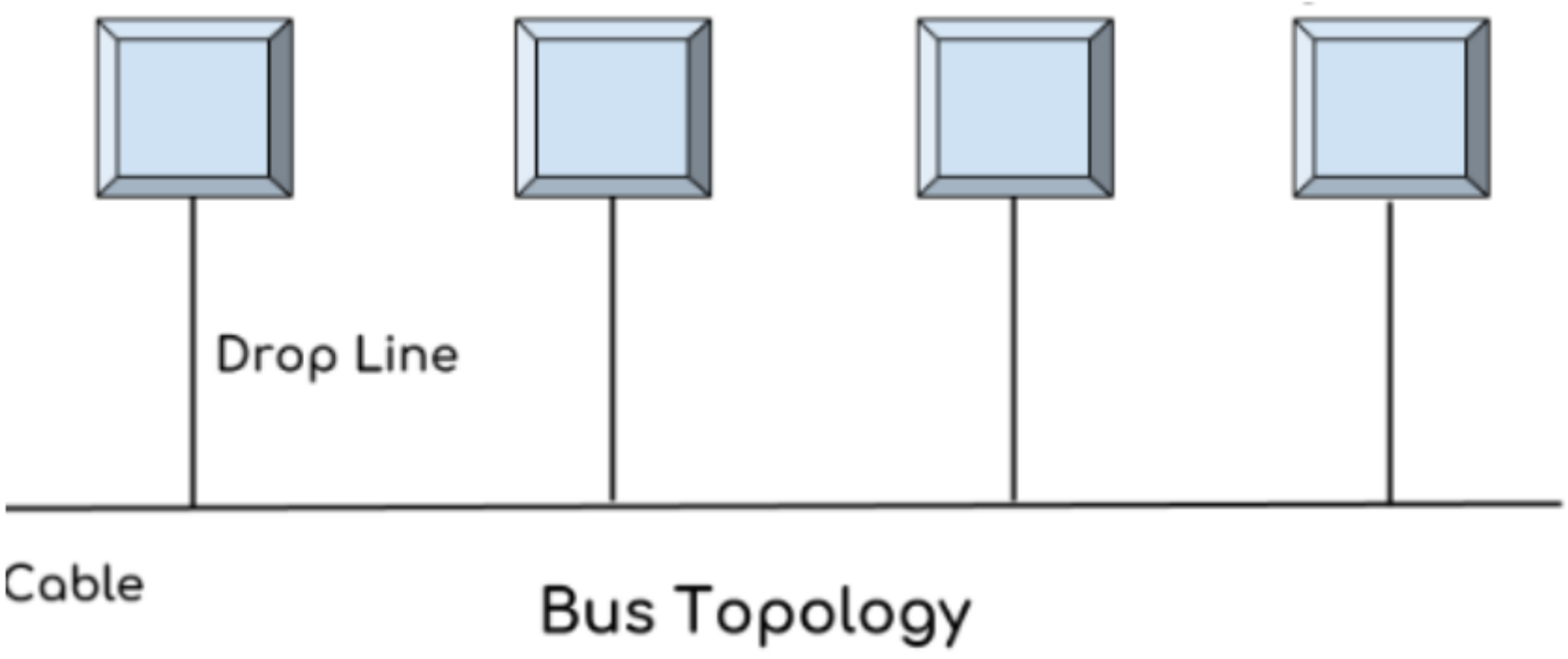
Fig: Star Topology

Topology

- **Bus Topology**
- In bus topology there is the main cable and all the devices are connected to this main cable through the drop lines.
- There is a device called tap that connects the drop line to the main cable.
- Since all the data is transmitted over the main cable, there is a limit on drop lines and the distance the main cable can have.
- **Advantages of bus topology**
- Easy installation, each cable needs to be connected with the backbone cable.
- Fewer cables are required than Mesh and star topology

Topology

- **Disadvantages of bus topology**
- Difficultly in fault detection.
- Not scalable as there is a limit on how many nodes you can connect with backbone cable.



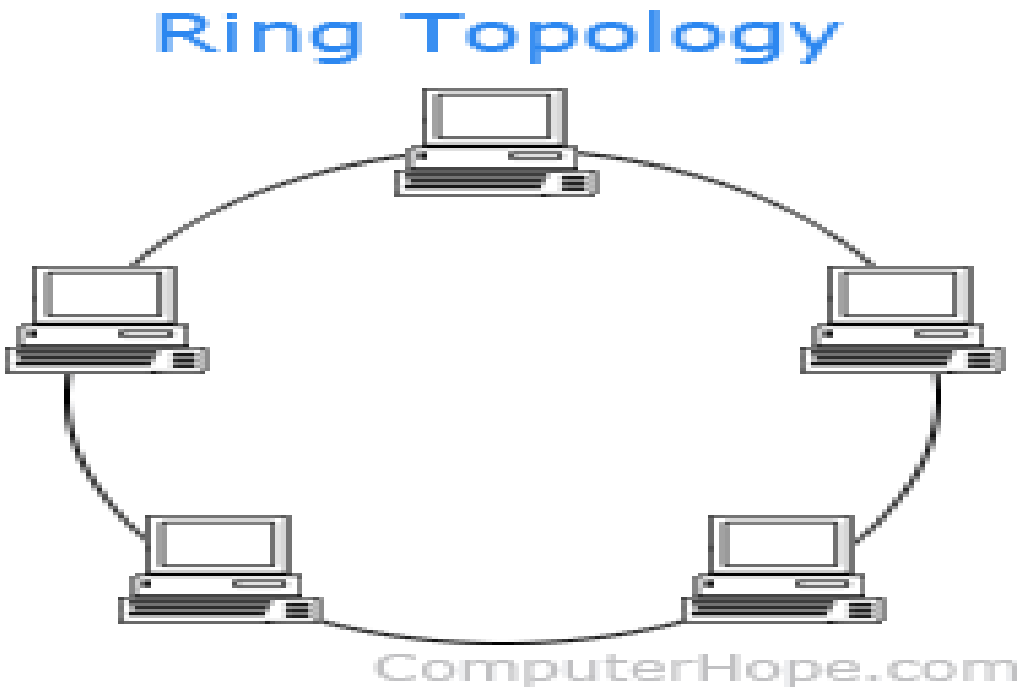
Topology

- **Ring Topology**
- In ring topology each device is connected with the two devices on either side of it.
- There are two dedicated point-to-point links a device has with the devices on either side of it.
- This structure forms a ring thus it is known as a ring topology.
- If a device wants to send data to another device then it sends the data in one direction, each device in ring topology has a repeater if the received data is intended for another device then the repeater forwards this data until the intended device receives it.

Topology

- **Advantages of Ring Topology**
- Easy to install.
- Managing is easier as to adding or removing a device from the topology only two links are required
  to be changed.
- **Disadvantages of Ring Topology**
- A link failure can fail the entire network as the signal will not travel forward due to failure.
- Data traffic issues, since all the data is circulating in a ring.

Topology



Open Systems Interconnection (OSI) Model

- An Open System is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture.
- The purpose of the OSI Model is to show how to facilitate communication between different systems without requiring changes to the underlying hardware and software logic.
- The OSI Model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable.
- The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems.
- It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network.

OSI Model

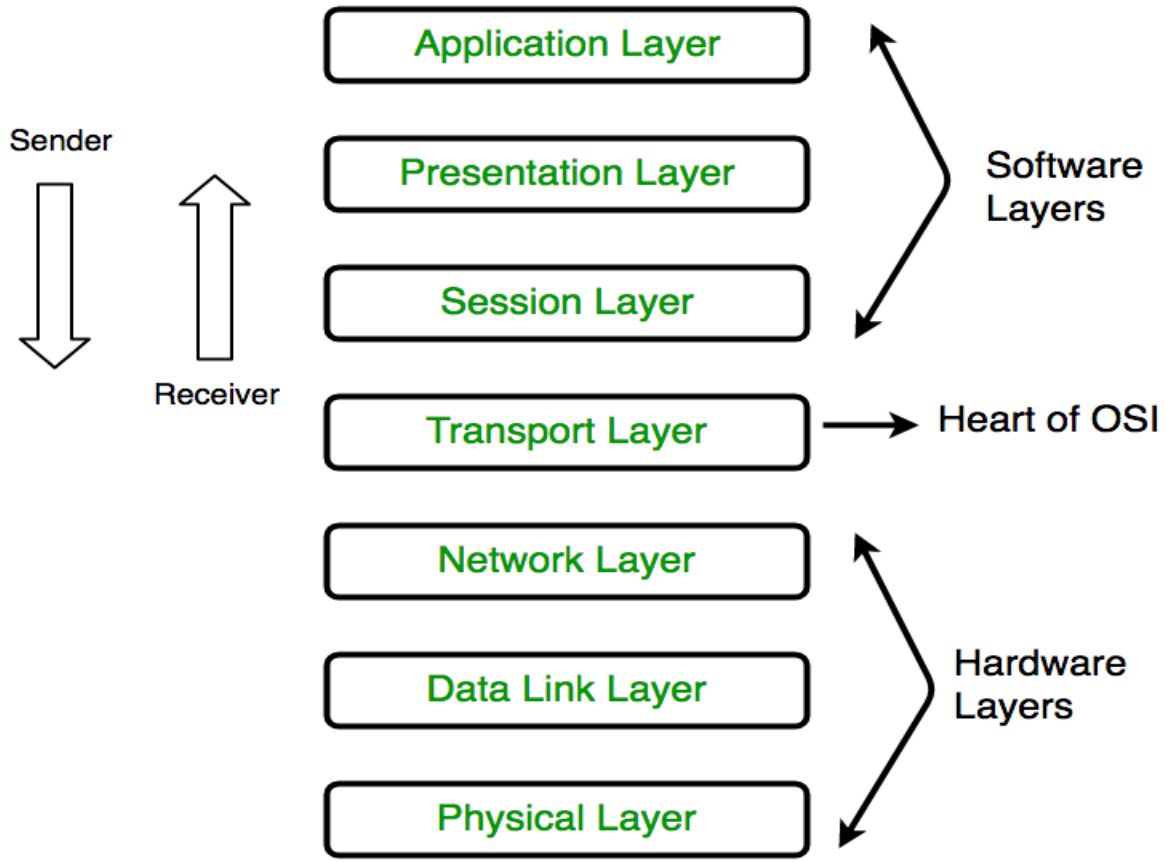


Fig: 7 layers of OSI Model

OSI Model

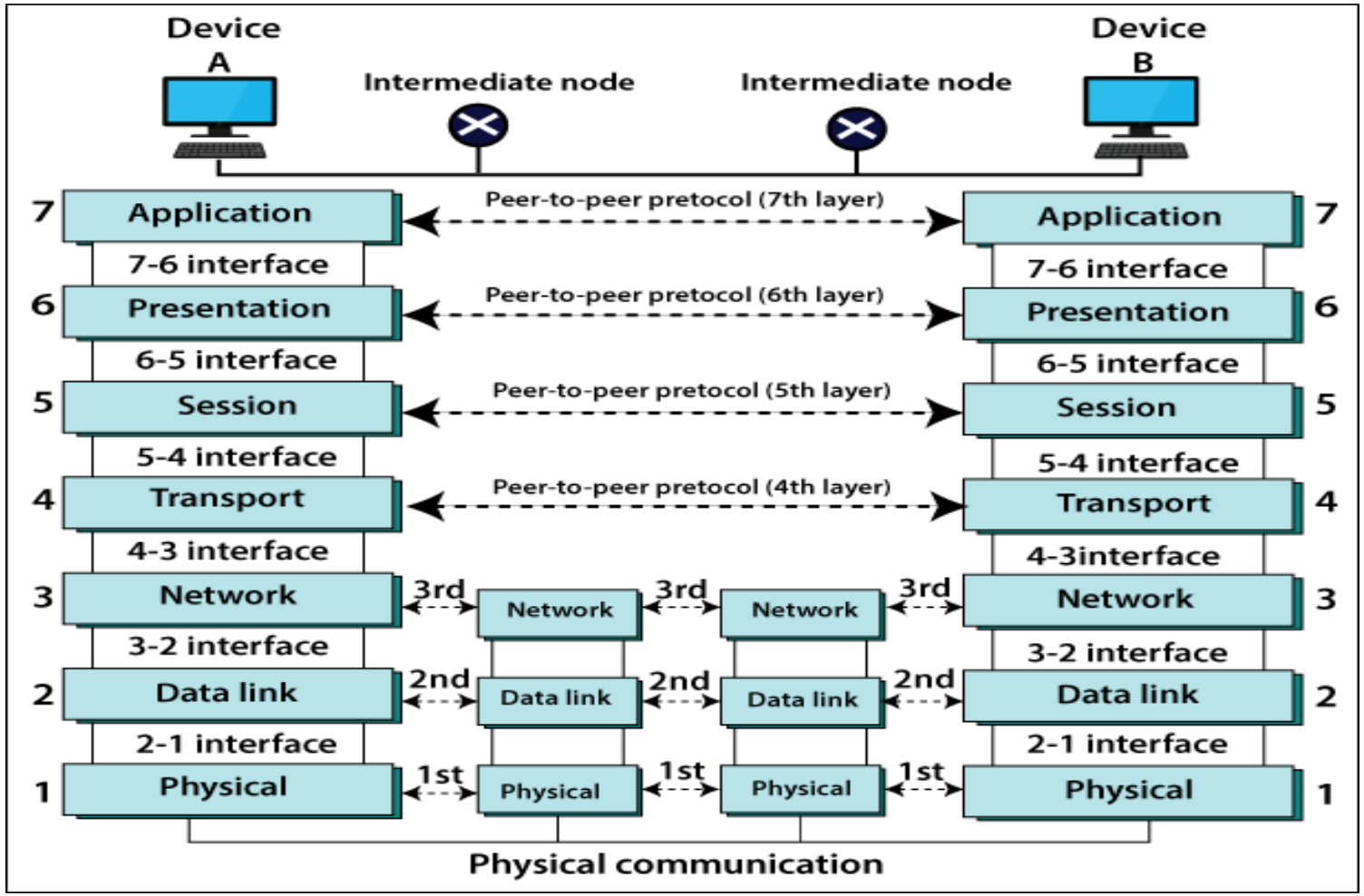


Fig: Interaction between two hosts using OSI Model

Layers of OSI Model

- **Layer 1: The Physical Layer**
- The first layer is the physical layer in the OSI model.
- This layer is also called a bit unit.
- The physical layer coordinates the functions needed to transmit a bit of stream to a physical medium.
- It is responsible for the actual physical connection between devices.
- The physical layer also describes whether the communication will be wireless or wired.
- The repeater is a device of the physical layer.

Physical Layer

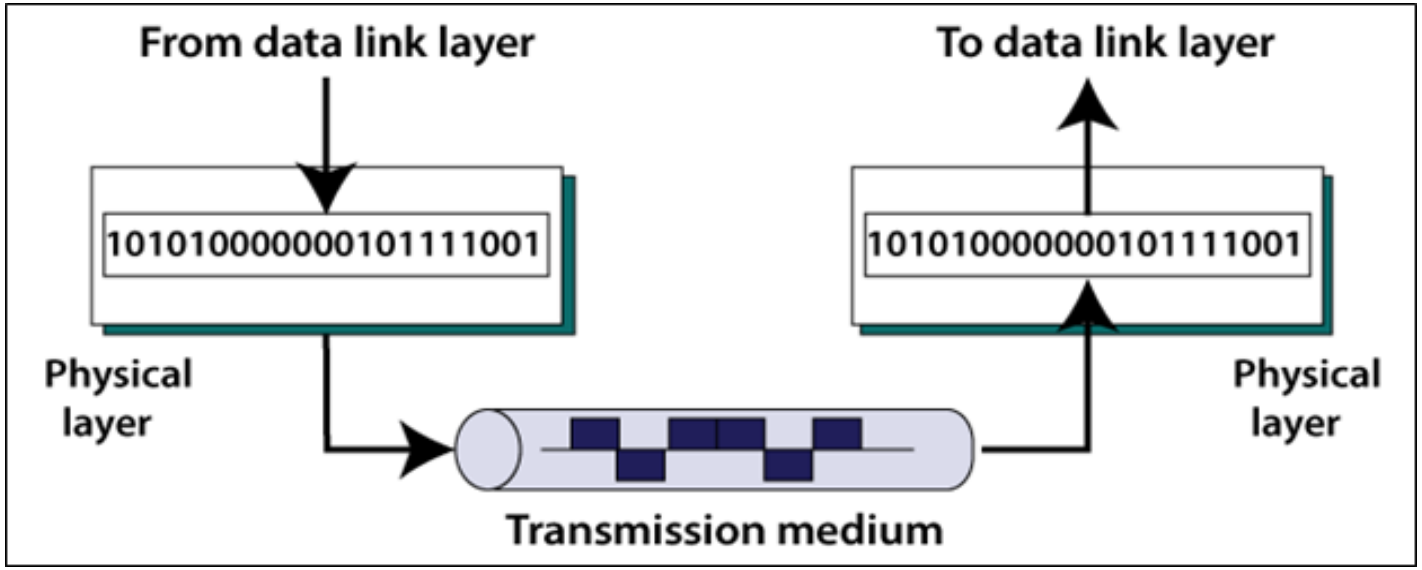


Fig: Physical Layer

Physical Layer

- **Major functions of the Physical Layers**
- **Physical characteristics of interface and media:** It defines the interface properties between devices and transmission devices. It also defines the type of transmission medium.
- **Line Configuration:** There are two types of line configuration Point-To-Point Configuration and Multipoint Configuration.
- **Data rate:** In data rate, the number of bits transmitted per second, is also defined by the physical layer. In other words, the physical layer determines how long the bit lasts.
- **Transmission mode:** It defines which transmission mode will be between two devices in the network.
- **Topology:** The physical layer defines how the different devices are organized in a network such as a bus, star, mesh, ring topology.

Layers of OSI Model

- **Layer 2: The Data Link Layer**
- The second layer is the Data Link layer in the OSI model.
- It is responsible for moving frames from one node to another.
- This layer is also called the Frame unit.
- In this layer, packets of data sent by the network layer are decoded and encoded.
- This layer also ensures the packets of data are error-free.

Data Link Layer

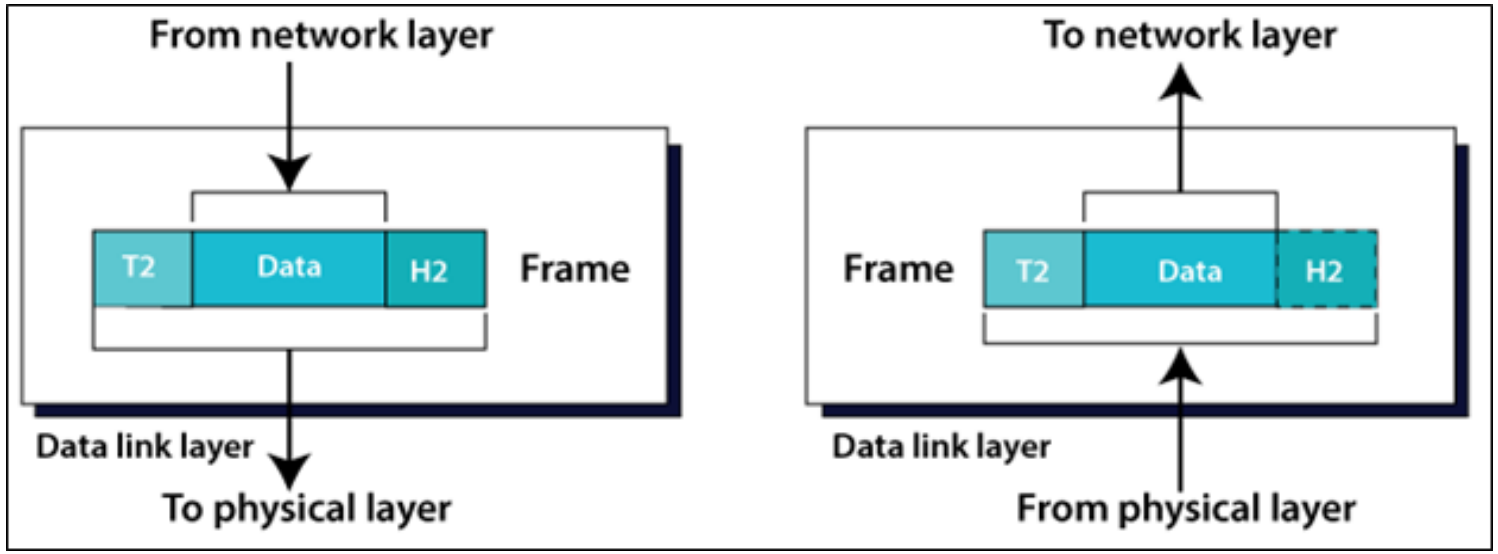


Fig : Data Link Layer

Data Link Layer

- **Major functions of the Data link layer**
- **Framing:** The data link layer divides the bit-stream received from the network layer into manageable pieces of data units called frames.
- **Physical Addressing :** Provide Device Address(MAC Address)
- **Flow control:** If the rate at which the receiver receives the data is less than the rate at which the data is produced at the sender end, the data link layer establishes a flow control mechanism to avoid overloading at the receiver end.
- **Error control:** It controls the error. CRC (cyclic redundancy check) is added to the end of the frame with the trailer so that the data is error-free.
- **Access Control:** When two or more devices are connected to the same link, the layer will determine which device is given access.

Layers of OSI Model

- **Layer 3: The Network Layer**
- The third layer is the Network layer in the OSI model.
- The data in the network layer is in the form of packets.
- It is responsible for the delivery of individual packets from the source to the destination.
- This layer is also called the packet unit.
- Switching and routing techniques are used in this layer.

Layers of OSI Model

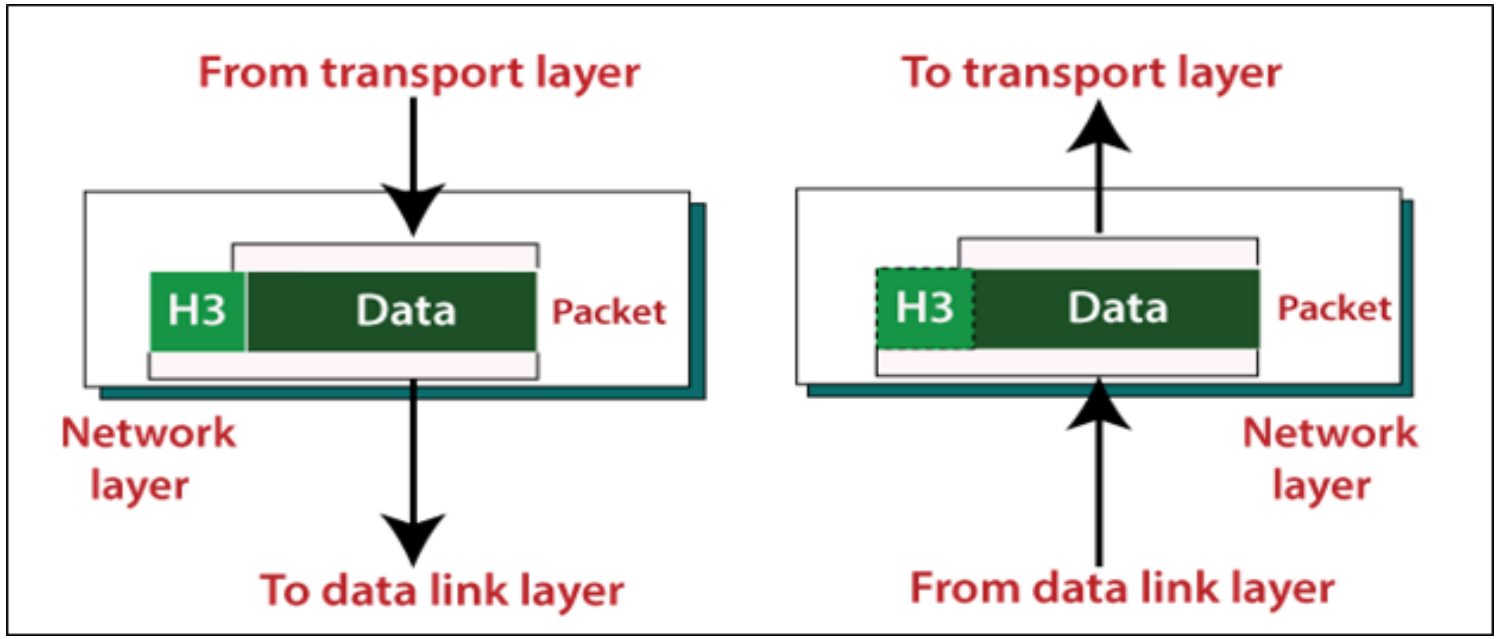


Fig : Network Layer

Layers of OSI Model

- **Major functions of the Network layer**
- **Routing:** When independent networks are connected to produce Internetworks, the connecting devices change the packets to their final end.
- One of the roles of this layer is to provide the mechanism.
- **Logical addressing:** The network layer defines a logical address so that each device on the Internet can be uniquely identified.
- The IP addresses of the sender and the receiver are placed in the header according to the network layer.
- This address distinguishes each device individually and generically.

Layers of OSI Model

- **Layer 4: The Transport Layer**
- The fourth layer is the Transport layer in the OSI model.
- It is responsible for the transfer of a message from one process to another.
- Although the network layer monitors the distribution of individual packets from source to destination, it does not recognize any connection between these packets.
- The transport layer also confirms a successful data transfer and re-transmits the data if an error is detected.

Layers of OSI Model

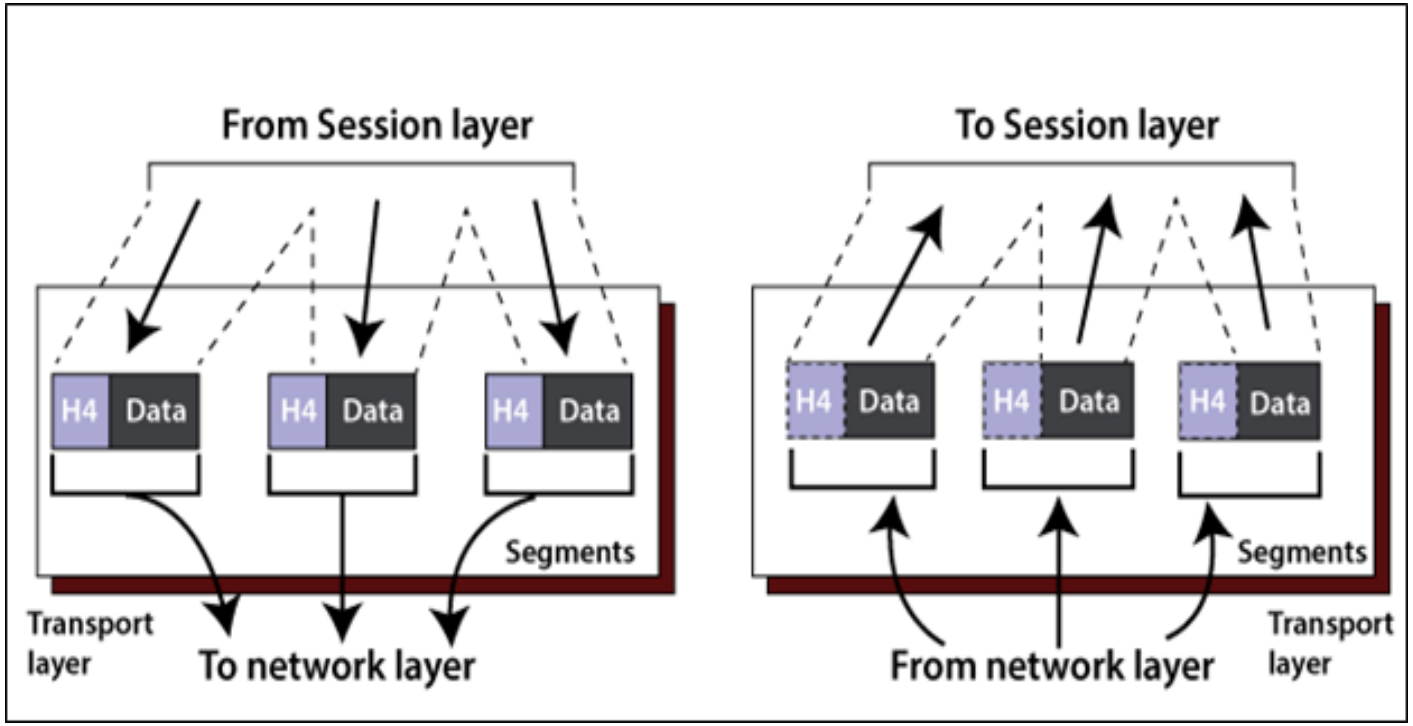


Fig : Transport Layer

Layers of OSI Model

- **Major functions of the Transport layer**
- **Segmentation and reassembly:** When this layer receives a message from the upper layers, it divides the message into many abstract segments.
- Each segment has a sequence number so that each segment can be easily identified.
- **Connection control:** It provides two types of connection: **Connection-oriented and Connectionless**.
- **Flow control:** The transport layer is responsible for flow control, similar to the data link layer.
- However, flow control in this layer is done end to end instead of a single link.
- **Error control:** The transport layer is responsible for error control, similar to the data link layer.
- However, error control in this layer is done end to end instead of a single link.

Layers of OSI Model

- **Layer 5: The Session Layer**
- The fifth layer is the Session layer in the OSI model, which controls connections between many computers.
- It manages, establishes, and terminates the session connection between two communication hosts.

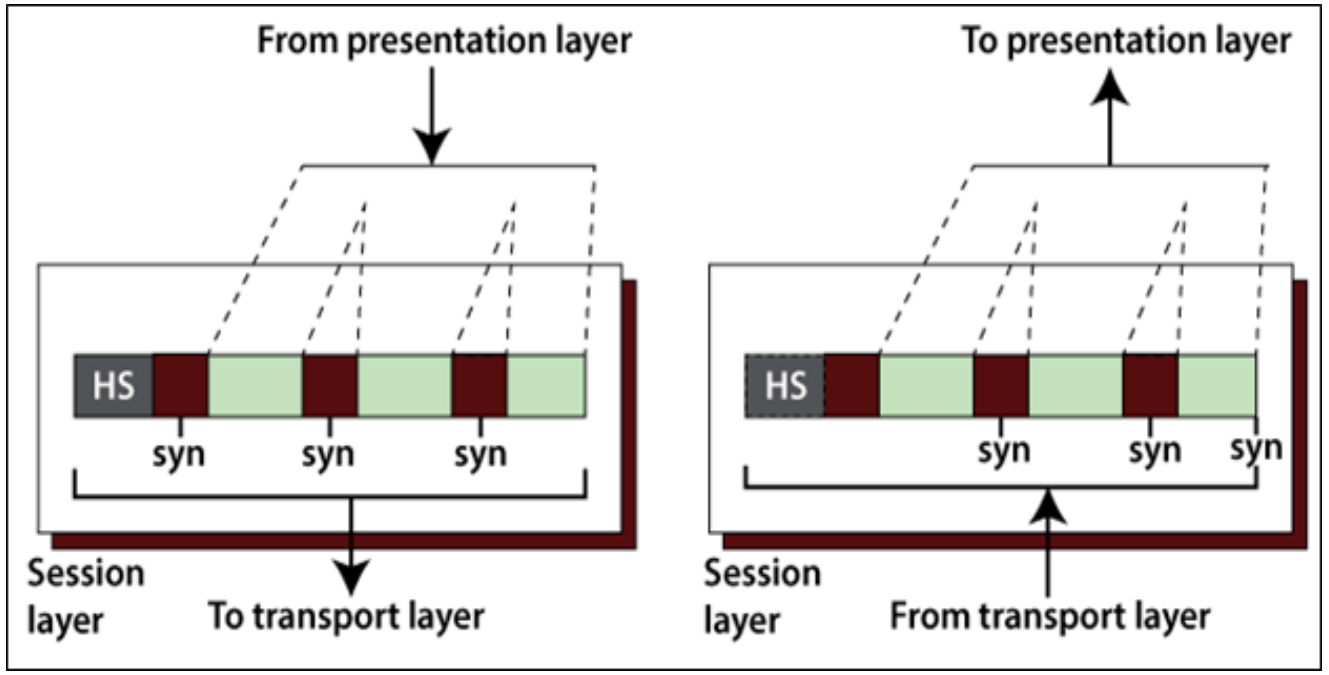


Fig: Session Layer

Layers of OSI Model

- **Major functions of the Session Layer**
- **Dialog control:** In the session layer, it allows two systems to enter a dialog that allows the communication between two processes in either half-duplex mode or full-duplex mode.
- **Synchronization:** It allows us to add the checkpoints into the stream of data.
- For example, suppose the system is sending a message of 1000 bits, it inserts the checkpoints after every 50 bits and to ensure that each 50 bits unit is received and acknowledged individually.
- In this case, if a crash happens during the transmission of 453 bit, that only needs to be a retransmission of 401 to 453. Previous of 401 bits are not required to re-sent.

Layers of OSI Model

- **Layer 6: The Presentation Layer**
- The sixth layer is the Presentation Layer in the OSI model.
- It deals with the syntax and semantics information which exchanges between two systems.

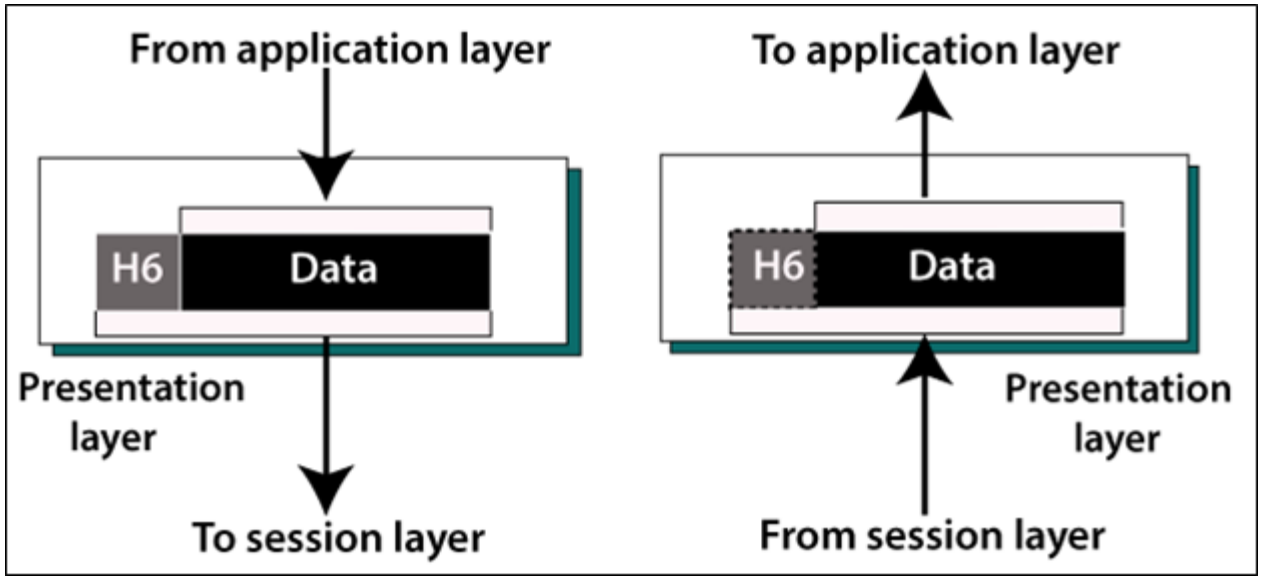


Fig : Presentation Layer

Layers of OSI Model

- **Major functions of the Presentation Layer**
- **Translation:** It converts a message to compatible bit-streams before being transmitted because various computers use various encoding methods.
- It is responsible for interoperability between these various encoding methods, which is changing the message into a standard format.
- **Encryption:** Encryption means to transform the original message into another form, that will not be readable by others.
- **Compression:** In Compression, it reduces the number of bits to be transmitted over the network.

Layers of OSI Model

- **Layer 7: The Application Layer**
- The seventh layer is the Application Layer in the OSI model.
- The end-user is the closest of application layer.
- This layer enables user access to the network. It allows remote logging into the application.

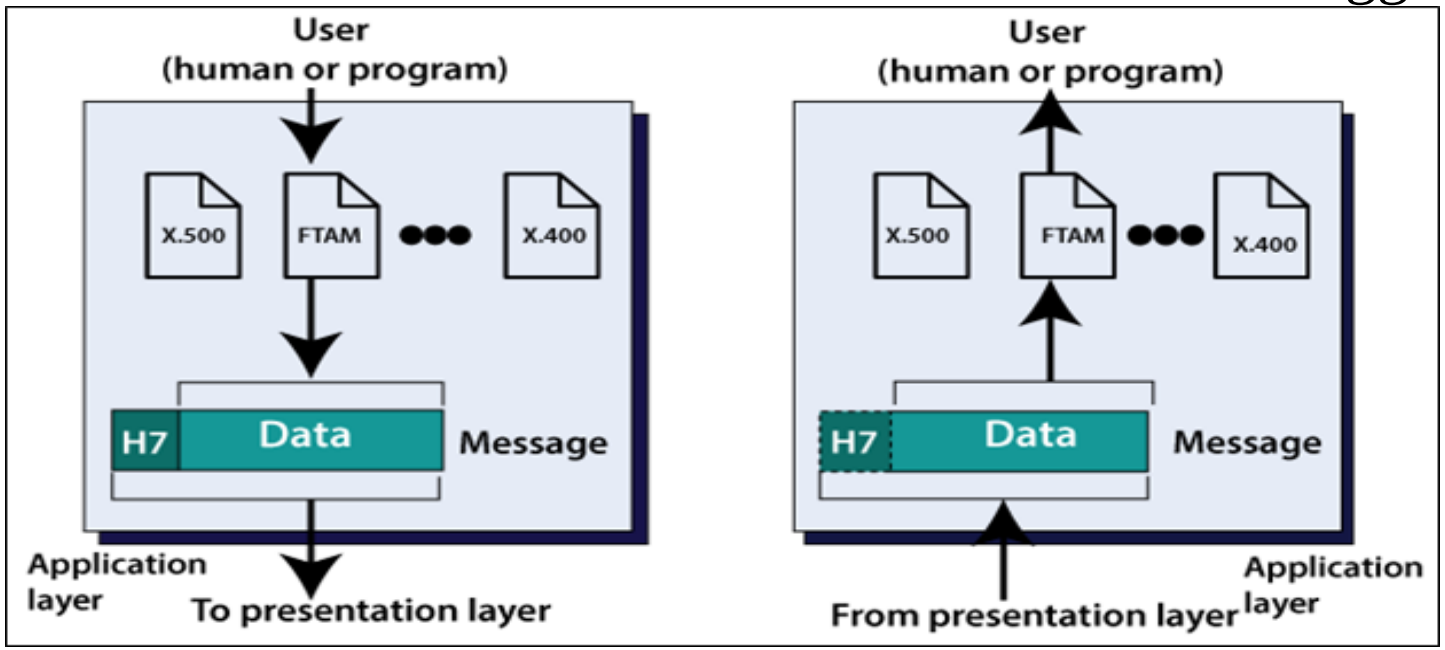


Fig : Application Layer

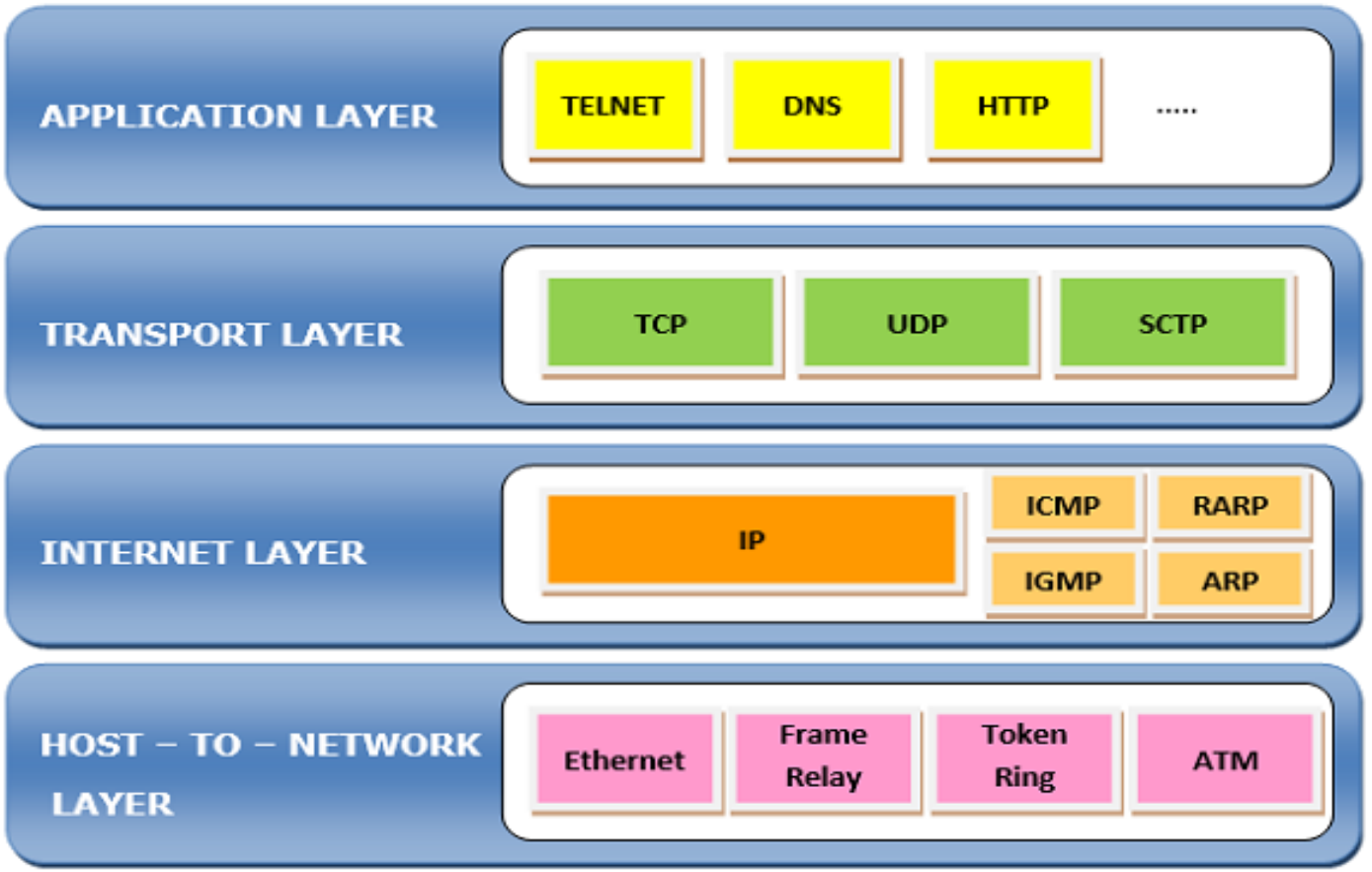
Layers of OSI Model

- **Major functions of the ApplicationLayer**
- **Network Virtual Terminal:** It’s a physical terminal to the software version. It provides remote host services.
- **File transfer, Access, and Management:** It allows a user to access, retrieve, and manage the files from a remote host.
- **Mail services:** It provides email forwarding and storage.

TCP/IP Model

- The TCP/IP model was developed prior to the OSI model.
- TCP/IP model is abbreviated by Transmission Control Protocol / Internet Protocol.
- The **OSI Model** we just looked at is just a reference/logical model.
- It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components.
- But when we talk about the TCP/IP model, it was designed and developed by the Department of Defense (DoD) in the 1960s and is based on standard protocols.
- It stands for Transmission Control Protocol/Internet Protocol.
- The **TCP/IP model** is a concise version of the OSI model.
- It contains four layers, unlike seven layers in the OSI model.

TCP/IP Model


APPLICATION LAYER
TELNET
DNS
HTTP
.....
TRANSPORT LAYER
TCP
UDP
SCTP
INTERNET LAYER
IP
ICMP
RARP
IGMP
ARP
HOST – TO – NETWORK LAYER
Ethernet
Frame Relay
Token Ring
ATM

Layers of TCP/IP Model

- **Layer 1: Network Access Layer**
- A network layer is the lowest layer of the TCP/IP model.
- A network layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model.
- It defines how the data should be sent physically through the network.
- This layer is mainly responsible for the transmission of the data between two devices on the same network.
- The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.
- The protocols used by this layer are ethernet, token ring, FDDI, X.25, frame relay.

Layers of TCP/IP Model

- **Layer 2: Internet Layer**
- An internet layer is the second layer of the TCP/IP model.
- An internet layer is also known as the network layer.
- The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.
- The internet layer defines an official packet format and protocol called IP (Internet Protocol).
- The job of the internet layer is to deliver IP packets where they are supposed to go
- Packet routing is clearly the major issue here, as is avoiding congestion.
- Other protocols are ARP(Address resolution Protocol),ICMP(Internet Control Message Protocol etc.

Layers of TCP/IP Model

- **Layer 3: Transport Layer**
- It is designed to allow peer entities on the source and destination hosts to carry on a conversation, just as in the OSI transport layer.
- Two end-to-end transport protocols :**TCP (Transmission Control Protocol)** is a reliable connection-oriented protocol that allows a byte stream originating on one machine to be delivered without error on any other machine in the internet.
- It fragments the incoming byte stream into discrete messages and passes each one on to the internet layer.
- At the destination, the receiving TCP process reassembles the received messages into the output stream.
- TCP also handles flow control to make sure a fast sender cannot swamp a slow receiver with more messages than it can handle.

Layers of TCP/IP Model

- UDP (User Datagram Protocol), is an unreliable, connectionless protocol for applications that do not want TCP's sequencing or flow control and wish to provide their own.
- It is also widely used for one-shot, client-server-type request-reply queries and applications in which prompt delivery is more important than accurate delivery, such as transmitting speech or video.

Layers of TCP/IP Model

- **Layer 4 :The Application Layer**
- The TCP/IP model does not have session or presentation layers.
- It contains all the higher-level protocols.
- The early ones included virtual terminal (TELNET), file transfer (FTP), and electronic mail (SMTP).
- The virtual terminal protocol allows a user on one machine to log onto a distant machine and work there.
- The file transfer protocol provides a way to move data efficiently from one machine to another.
- Electronic mail was originally just a kind of file transfer, but later a specialized protocol (SMTP) was developed for it.

Layers of TCP/IP Model

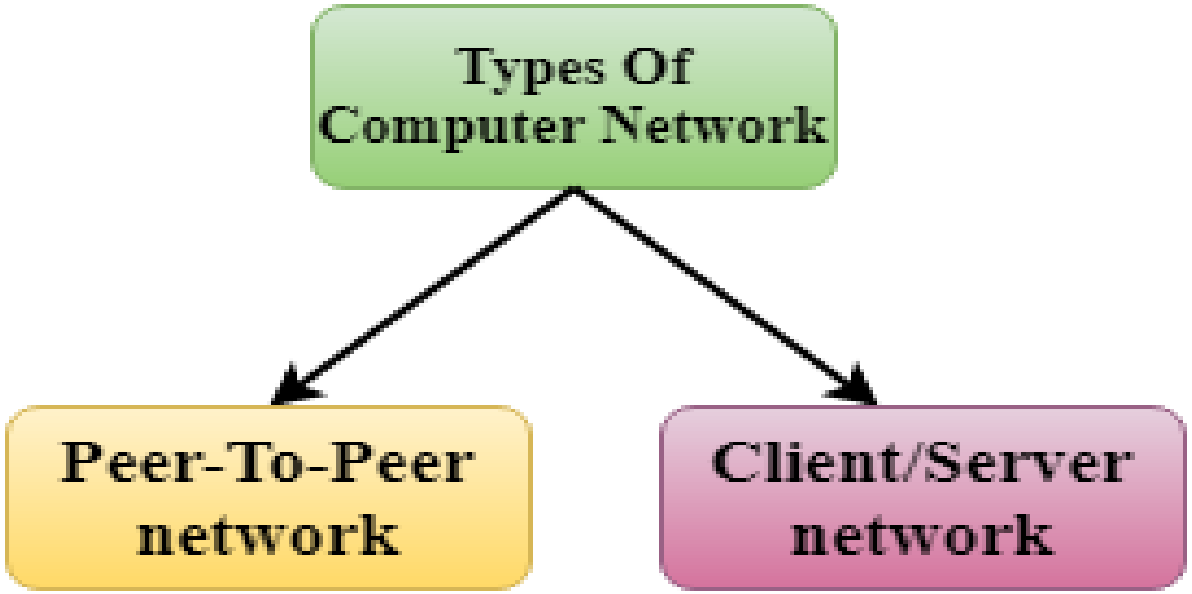
- Many other protocols have been added to these over the years:
- The Domain Name System (DNS) for mapping host names onto their network addresses.
- NNTP, the protocol for moving USENET news articles around
- HTTP, the protocol for fetching pages on the World Wide Web.

Comparison of OSI and TCP/IP Model

OSI Model	TCP/IP Model
It is developed by ISO (International Standard Organization)	It is developed by ARPANET (Advanced Research Project Agency Network).
OSI model provides a clear distinction between interfaces, services, and protocols.	TCP/IP doesn't have any clear distinguishing points between services, interfaces, and protocols.
OSI refers to Open Systems Interconnection.	TCP refers to Transmission Control Protocol.
OSI uses the network layer to define routing standards and protocols.	TCP/IP uses only the Internet layer.
OSI follows a vertical approach.	TCP/IP follows a horizontal approach.
OSI layers have seven layers.	TCP/IP has four layers.
In the OSI model, the transport layer is only connection-oriented.	A layer of the TCP/IP model is both connection-oriented and connectionless.
In the OSI model, the data link layer and physical are separate layers.	In TCP, physical and data link are both combined as a single host-to-network layer.
Session and presentation layers are a part of the OSI model.	There is no session and presentation layer in the TCP model.
It is defined after the advent of the Internet.	It is defined before the advent of the internet.
The minimum size of the OSI header is 5 bytes.	The minimum header size is 20 bytes.

Network Architecture

- Computer Network Architecture is defined as the physical and logical design of the software, hardware, protocols, and media for the transmission of data.
- Simply we can say how computers are organized and how tasks are allocated to the computer.



Network Architecture

- **Peer-To-Peer network**
- Peer-To-Peer network is a network in which all the computers are linked together with equal privilege and responsibilities for processing the data.
- Peer-To-Peer network is useful for small environments, usually up to 10 computers.
- Peer-To-Peer network has no dedicated server.
- Special permissions are assigned to each computer for sharing the resources, but this can lead to a problem if the computer with the resource is down.

Network Architecture

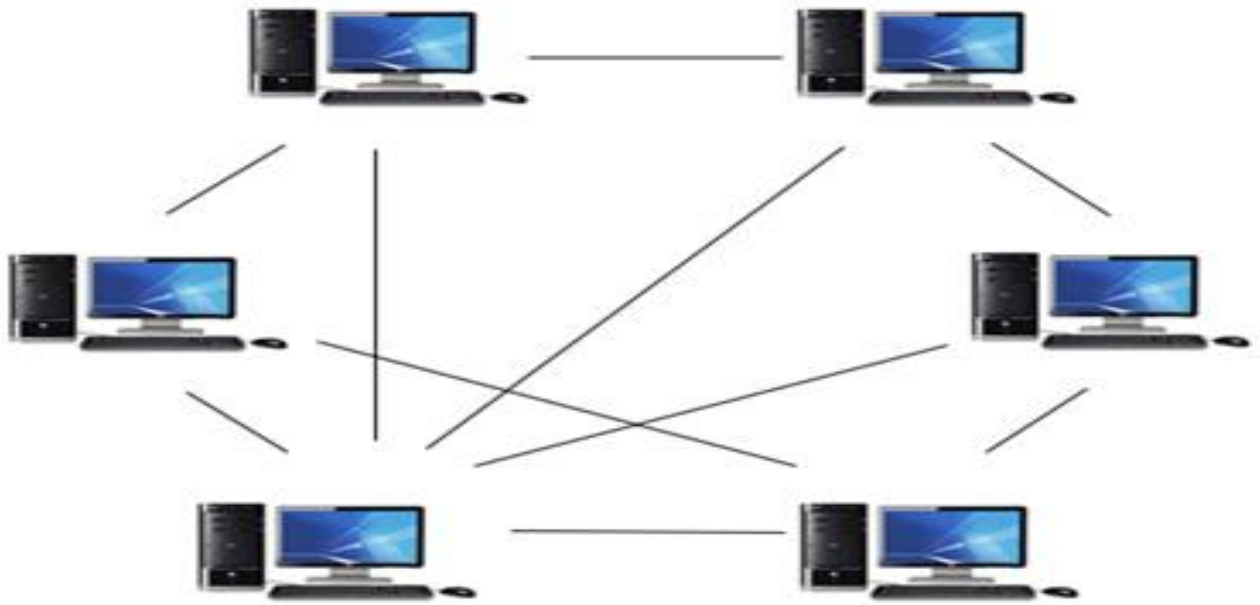


Fig: Peer to Peer Architecture

Network Architecture

- **Advantages Of Peer-To-Peer Network**
- It is less costly as it does not contain any dedicated server.
- If one computer stops working, other computers will not stop working.
- It is easy to set up and maintain as each computer manages itself.
- **Disadvantages Of Peer-To-Peer Network**
- In the case of a Peer-To-Peer network, it does not contain a centralized system .
- Therefore, it cannot back up the data as the data is different in different locations.
- It has a security issue as the device is managed itself.

Network Architecture

- **Client/Server Network**
- Client/Server network is a network model designed for the end-users called clients, to access the resources such as songs, video, etc. from a central computer known as Server.
- The central controller is known as a **server** while all other computers in the network are called **clients**.
- A server performs all the major operations such as security and network management.
- A server is responsible for managing all the resources such as files, directories, printers, etc.
- All the clients communicate with each other through a server.
- For example, if client1 wants to send some data to client 2, then it first sends the request to the server for permission.
- The server sends the response to client 1 to initiate its communication with client 2.

Network Architecture

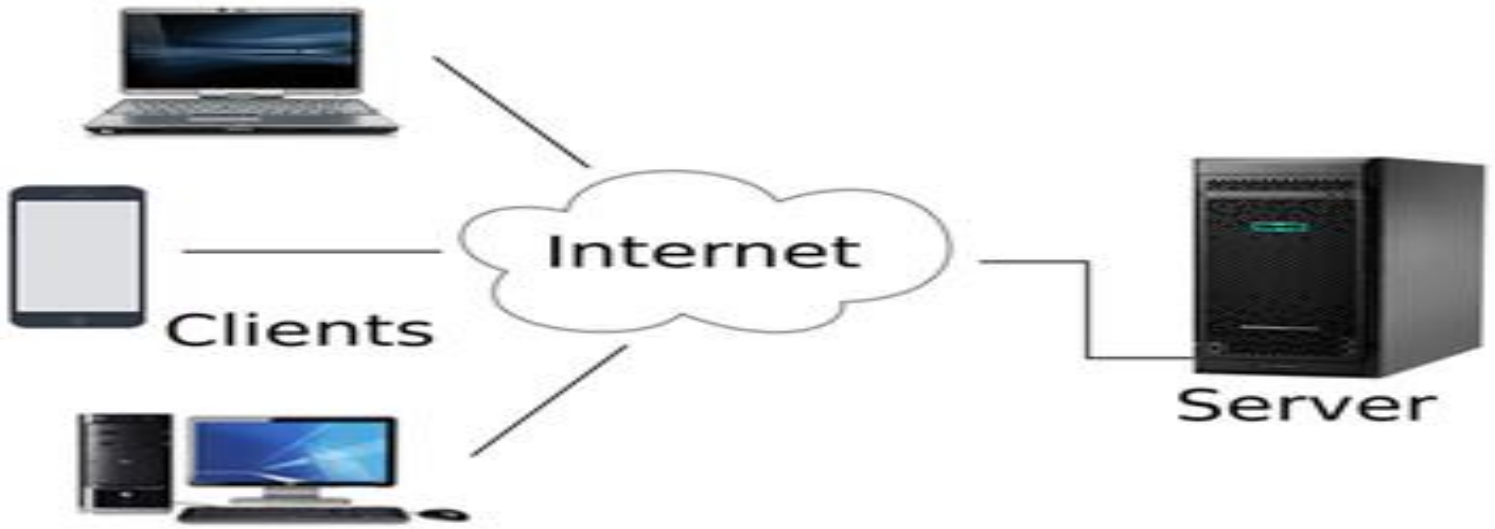


Fig : Client-Server Architecture

Network Architecture

- **Advantages Of Client/Server network**
- A Client/Server network contains the centralized system. Therefore we can back up the data easily.
- A Client/Server network has a dedicated server that improves the overall performance of the whole system.
- Security is better in Client/Server network as a single server administers the shared resources.
- It also increases the speed of the sharing resources.
- **Disadvantages Of Client/Server network**
- Client/Server network is expensive as it requires the server with large memory.
- A server has a Network Operating System(NOS) to provide the resources to the clients, but the cost of NOS is very high.
- It requires a dedicated network administrator to manage all the resources.

Network Architecture

BASIS FOR COMAPAISON	CLIENT-SERVER	PEER-TO-PEER
Basic	There is a specific server and specific clients connected to the server.	Clients and server are not distinguished; each node act as client and server.
Service	The client request for service and server respond with the service.	Each node can request for services and can also provide the services.
Focus	Sharing the information.	Connectivity.
Data	The data is stored in a centralized server.	Each peer has its own data.
Server	When several clients request for the services simultaneously, a server can get bottlenecked.	As the services are provided by several servers distributed in the peer-to-peer system, a server in not bottlenecked.
Expense	The client-server are expensive to implement.	Peer-to-peer are less expensive to implement.
Stability	Client-Server is more stable and scalable.	Peer-toPeer suffers if the number of peers increases in the system.

IEEE standards

IEEE 802 Standards Working Groups

Number	Topic
802.1	Overview and architecture of LANs
802.2 ↓	Logical link control
802.3 *	Ethernet
802.4 ↓	Token bus (was briefly used in manufacturing plants)
802.5	Token ring (IBM's entry into the LAN world)
802.6 ↓	Dual queue dual bus (early metropolitan area network)
802.7 ↓	Technical advisory group on broadband technologies
802.8 †	Technical advisory group on fiber optic technologies
802.9 ↓	Isochronous LANs (for real-time applications)
802.10 ↓	Virtual LANs and security
802.11 *	Wireless LANs
802.12 ↓	Demand priority (Hewlett-Packard's AnyLAN)
802.13	Unlucky number. Nobody wanted it
802.14 ↓	Cable modems (defunct: an industry consortium got there first)
802.15 *	Personal area networks (Bluetooth) 802.15.4 ZigBee
802.16 *	Broadband wireless
802.17	Resilient packet ring

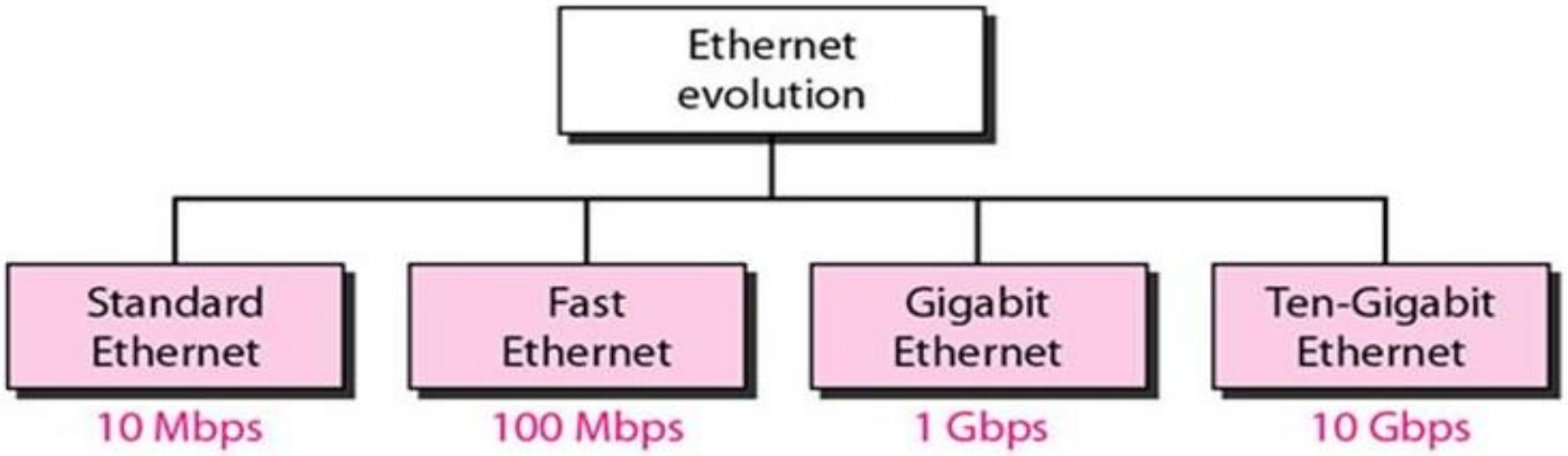
Figure 1-38. The important ones are marked with *. The ones marked with ↓ are hibernating. The one marked with † gave up.

Overview of IEEE Standard 802 for LANS and MANS

- IEEE 802 is an Institute of Electrical and Electronics Engineers (IEEE) standard set that covers the physical and data link layers of the Open Systems Interconnection (OSI) model.
- It defines standards and protocols for wired local area networks (WLAN), metropolitan area networks (MAN) and wireless networks; defines characteristics, operating procedures, protocols and services for networks that carry variable sized packets and specifies the development and handling of compatible devices and equipment.
- IEEE 802 is comprised of standards with separate working groups that regulate different communication networks, including IEEE 802.1 for bridging (bottom sublayer), 802.2 for Logical link (upper sublayer), 802.3 for Ethernet, 802.5 for token ring, 802.11 for Wi-Fi, 802.15 for Wireless Personal area networks, 802.15.1 for Bluetooth, 802.16 for Wireless Metropolitan Area Networks etc.

Overview of IEEE Standard 802 for LANS and MANS

Ethernet:
The original Ethernet was created in 1976 and since then, it has gone through four generations.

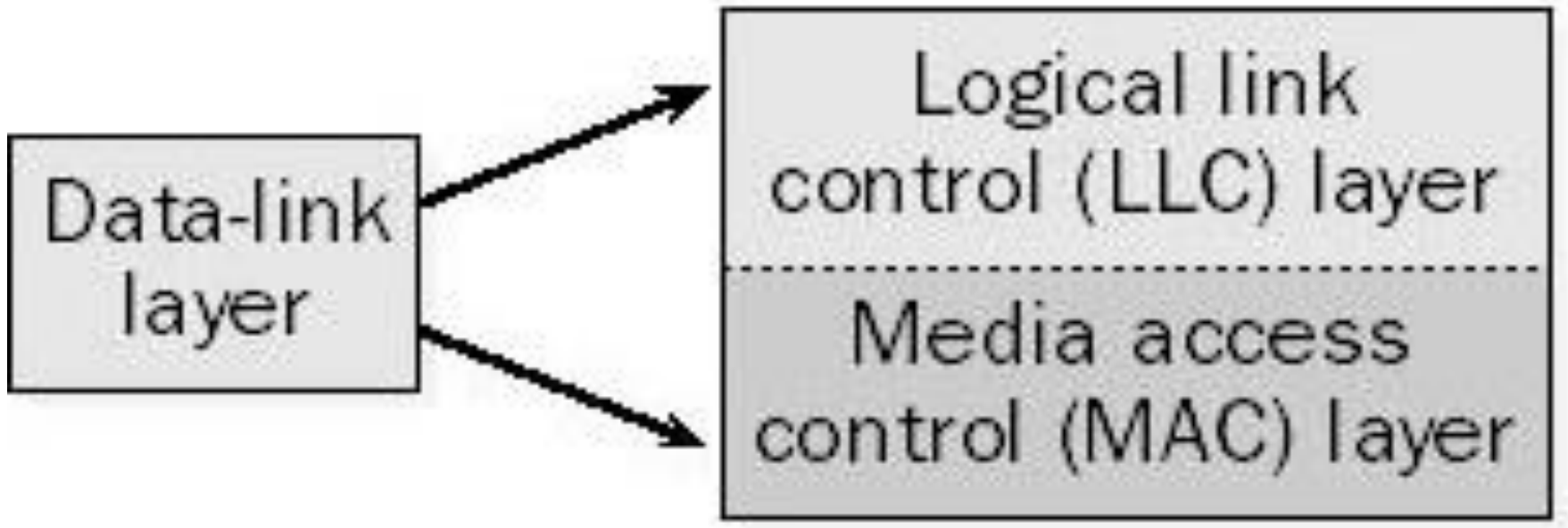


Overview of IEEE Standard 802 for LANS and MANS

- Ethernet is a family of computer networking technologies commonly used in local area networks (LAN), metropolitan area networks (MAN), and wide area networks (WAN).
- Systems using Ethernet communication divide data streams into packets, which are known as frames.
- Frames include source and destination address information, as well as mechanisms used to detect errors in transmitted data and retransmission requests.
- An Ethernet cable is the physical, encased wiring over which the data travels.
- Compared to wireless LAN technology, Ethernet is typically less vulnerable to disruptions.
- It can also offer a greater degree of network security and control than wireless technology, as devices must connect using physical cabling, making it difficult for outsiders to access network data or hijack bandwidth for unsanctioned devices.

MAC Sublayer

- For LANs, the Project 802 standards of the Institute of Electrical and Electronics Engineers (IEEE) separate the data-link layer into two sub layers.



MAC Sublayer

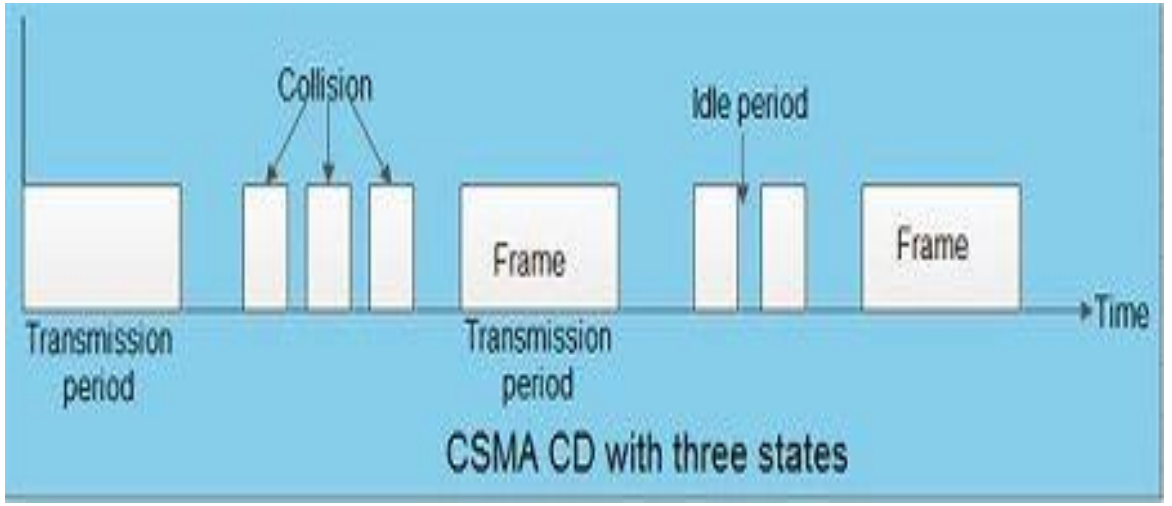
- Logical link control(LLC) layer is the upper part of the two layers.
- Responsible for flow control, error correction, and re-sequencing functions for connection-oriented and connectionless communication which is been already discussed.
- MAC layer is responsible to provide a method for stations to gain access to the medium.

Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

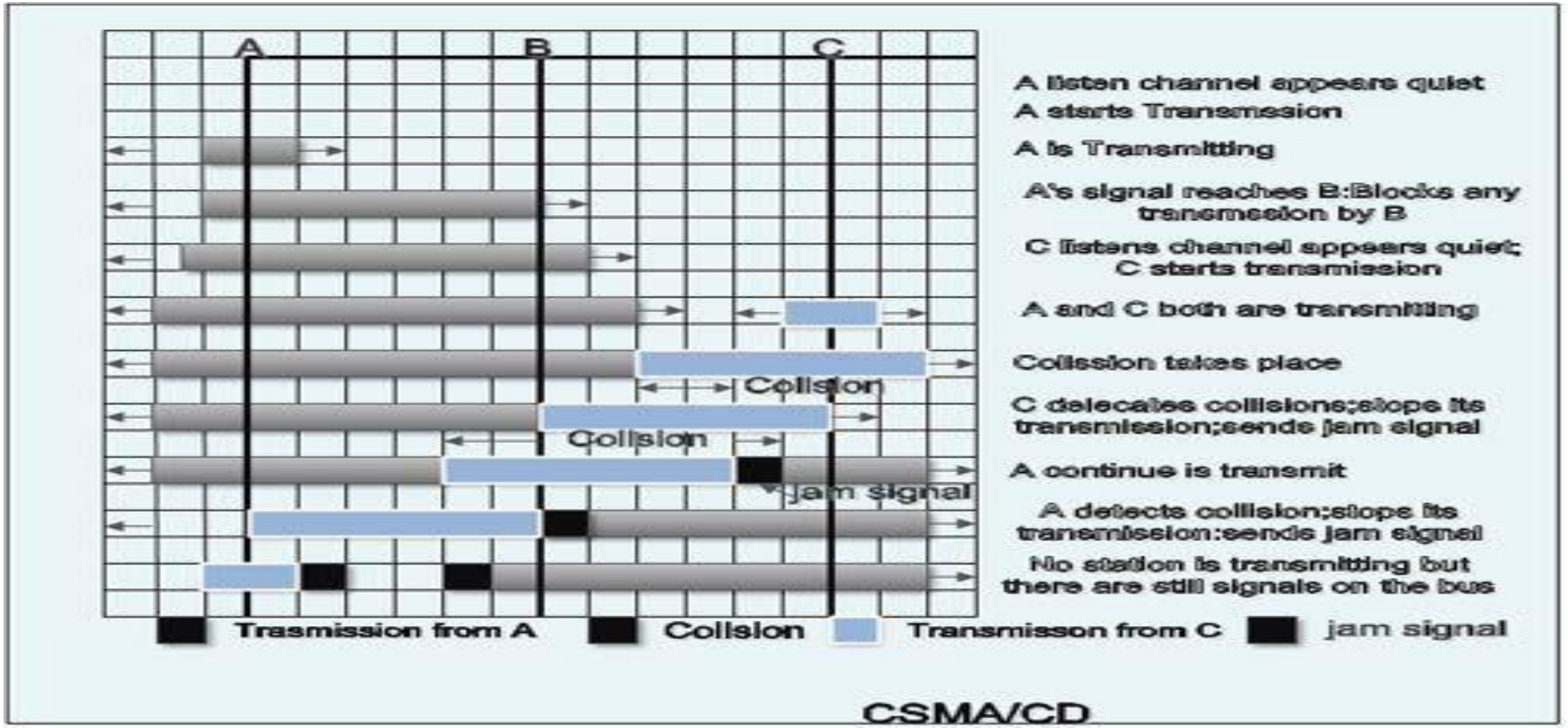
- **CSMA/CD**
- To reduce the impact of collisions on the network performance, Ethernet uses an algorithm called CSMA with Collision Detection (CSMA / CD.
- CSMA/CD is a protocol in which the station senses the carrier or channel before transmitting frame just as in persistent and non-persistent CSMA.
- If the channel is busy, the station waits.
- It listens at the same time on communication media to ensure that there is no collision with a packet sent by another station.
- In a collision, the issuer immediately cancel the sending of the package.
- This allows to limit the duration of collisions: we do not waste time to send a packet complete if it detects a collision.

Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

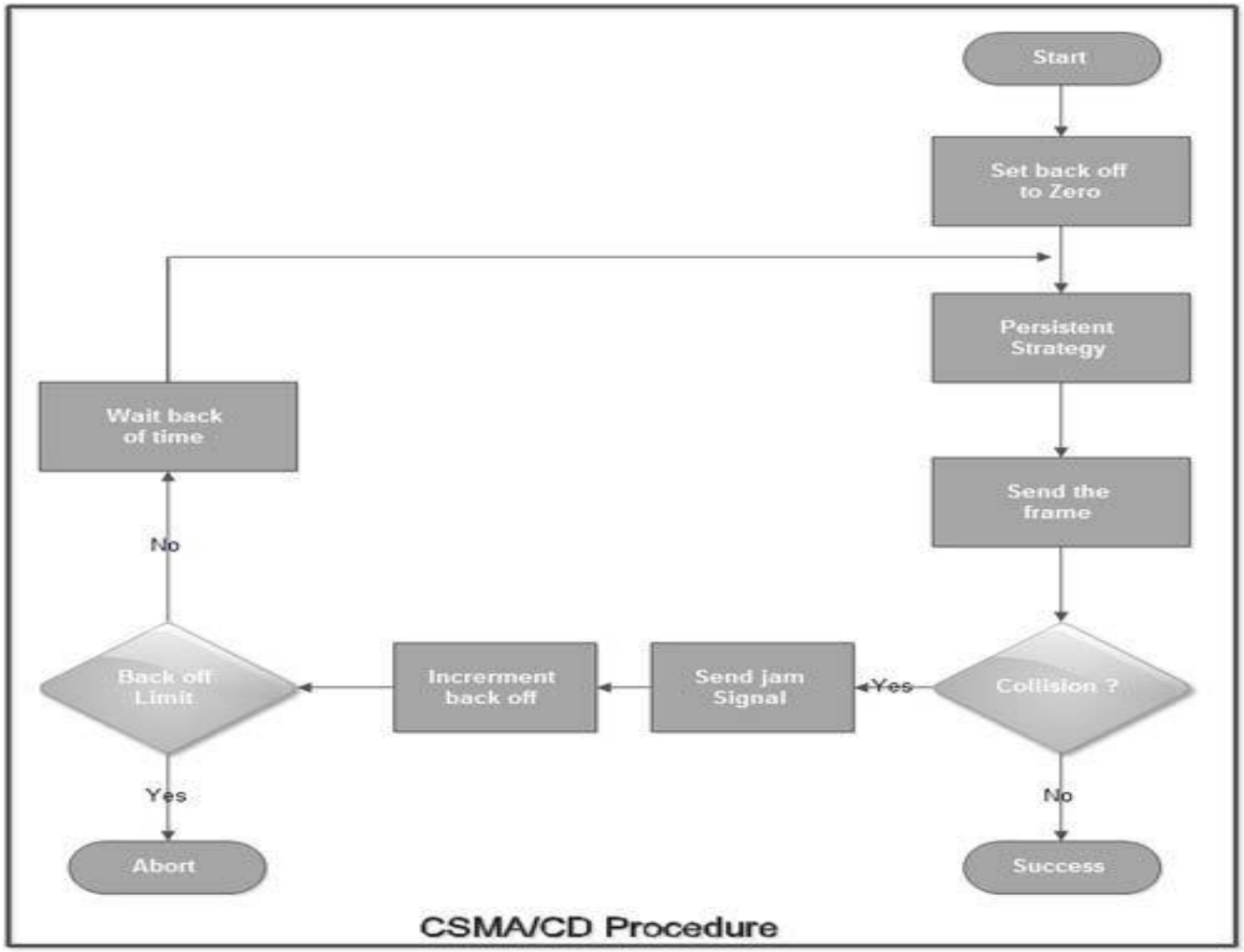
- After a collision, the transmitter waits again silence, and again, he continued his hold for a random number; but this time the random number is nearly double the previous one: it is this called back-off (that is to say, the “decline”) exponential.
- In fact, the window collision is simply doubled (unless it has already reached a maximum).
- From a packet is transmitted successfully, the window will return to its original size.



Carrier Sense Multiple Access with Collision Detection (CSMA/CD)



Carrier Sense Multiple Access with Collision Detection (CSMA/CD)



Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

- **CSMA/CD Procedure:**
- The station that has a ready frame sets the backoff parameter to zero.
- Then it senses the line using one of the persistent strategies.
- If then sends the frame. If there is no collision for a period corresponding to one complete frame, then the transmission is successful.
- Otherwise the station sends the jamming signal to inform the other stations about the collision.
- The station then increments the backoff time and waits for a random backoff time and sends the frame again.
- If the backoff has reached its limit then the station aborts the transmission.
- *CSMA/CD* is used for the traditional Ethernet.
- *CSMA/CD* is an important protocol. IEEE 802.3 (Ethernet) is an example of *CSMACD*. It is an international standard.
- The MAC sublayer protocol does not guarantee reliable delivery. Even in absence of collision, the receiver may not have copied the frame correctly.

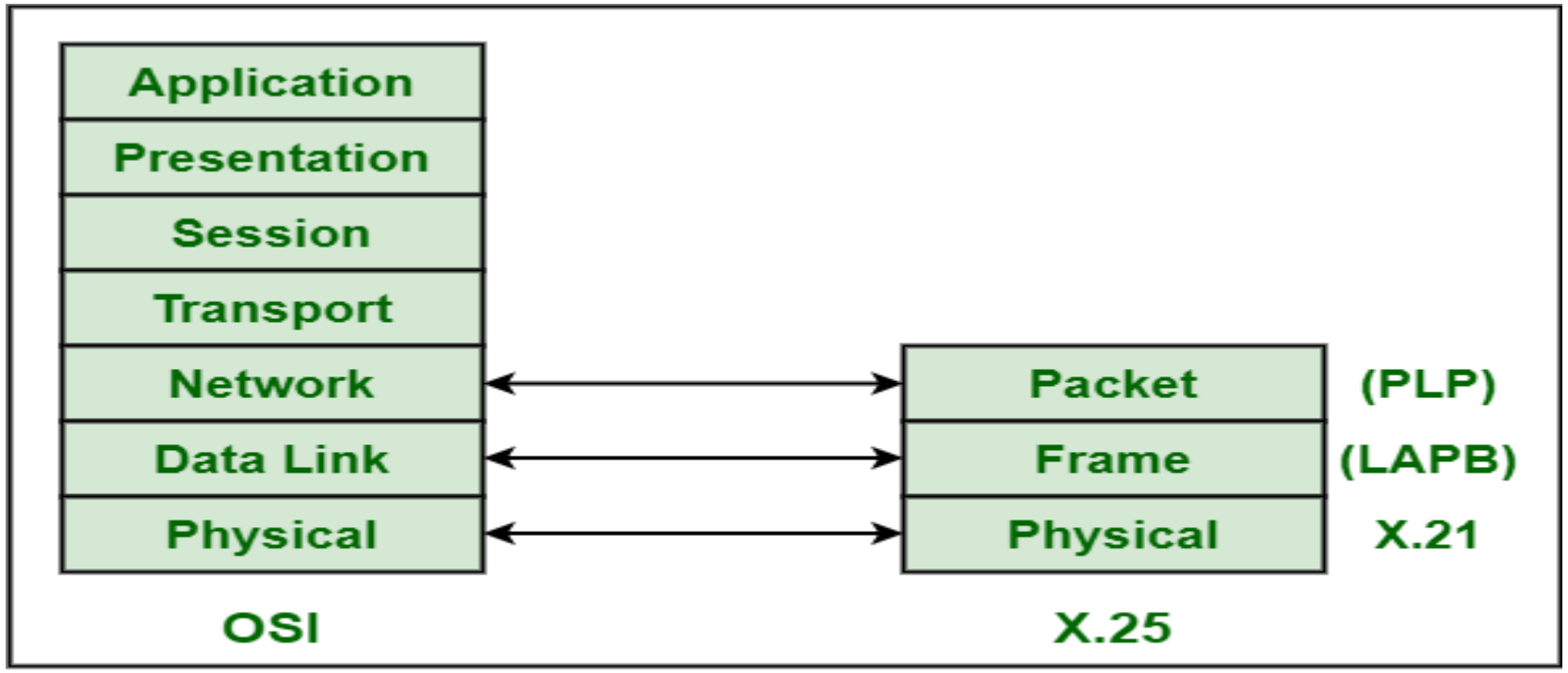
X.25, Frame Relay, ATM

- **X.25**
- X.25 is a protocol suite defined by ITU-T for packet-switched communications over WAN (Wide Area Network).
- It was originally designed for use in the 1970s and became very popular in the 1980s.
- Presently, it is used for networks for ATMs and credit card verification.
- It allows multiple logical channels to use the same physical line.
- It also permits data exchange between terminals with different communication speeds.

X.25, Frame Relay, ATM

- **X.25 has three protocol layers**
- **Physical Layer:** It lays out the physical, electrical and functional characteristics that interface between the computer terminal and the link to the packet switched node.
- X.21 physical implementer is commonly used for the linking.
- **Data Link Layer:** It comprises the link access procedures using Link Access Procedure Balanced(LAPB) for exchanging data over the link.
- This service ensures a bit-oriented, error-free, and ordered delivery of frames.
- **Packet Layer:** This layer defines the format of data packets and the procedures for control and transmission of the data packets.

X.25, Frame Relay, ATM



X.25 Layer Mapping with OSI Model

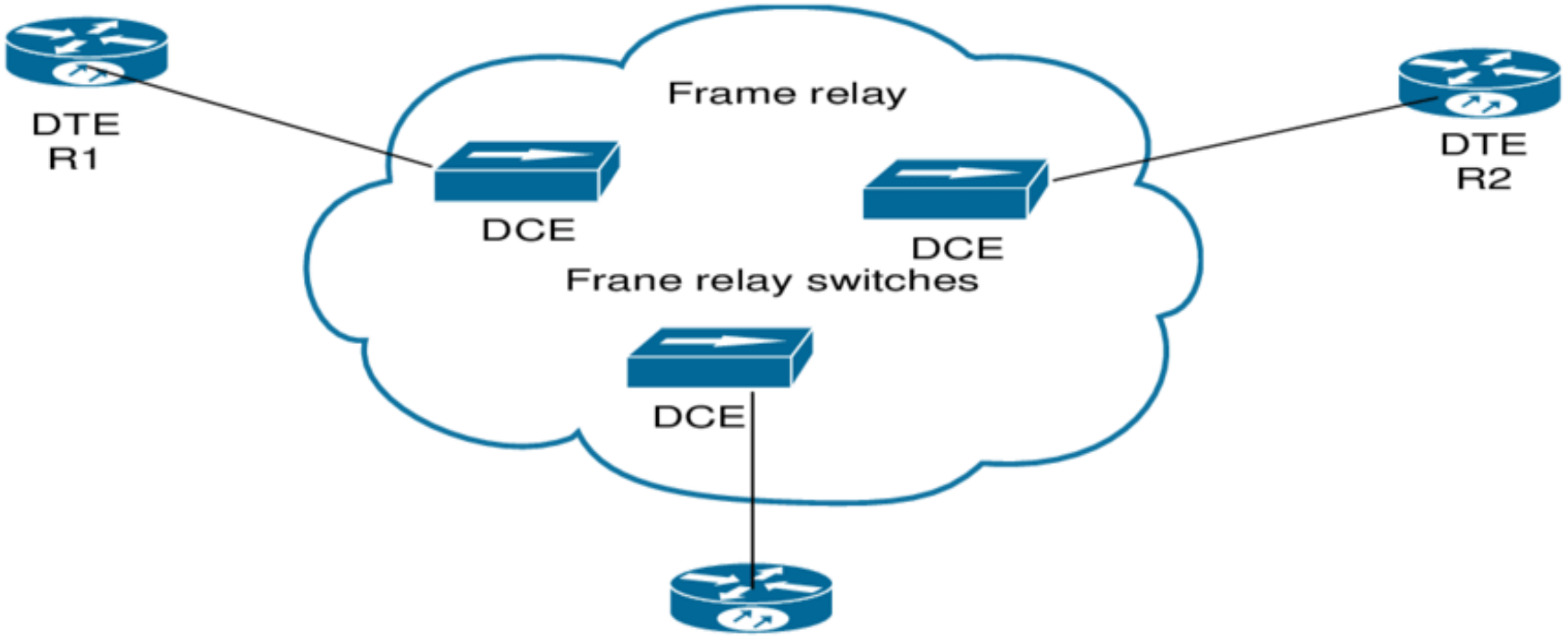
X.25, Frame Relay, ATM

- **Frame Relay**
- Frame Relay is a packet-switched communication service from LANs (Local Area networks) to backbone networks and WANs.
- It operates at two layers: the physical layer and the data link layer.
- It supports all standard physical layer protocols.
- It is mostly implemented at the data link layer.
- Frame Relay operates at a higher speed (1.544 Mbps and recently 44.376 Mbps).
- Frame Relay allows bursty data.
- Frame Relay allows a frame size of 9000 bytes, which can accommodate all local-area network frame sizes.
- Frame Relay has error detection at the data link layer only ie. there is no flow control or error control.

X.25, Frame Relay, ATM

- Frame Relay uses virtual circuits to connect a single router to multiple remote sites.
- In most cases, permanent virtual circuits are used, i.e. a fixed network-assigned circuit is used through which the user sees a continuous uninterrupted line.
- However, switched virtual circuits may also be used.

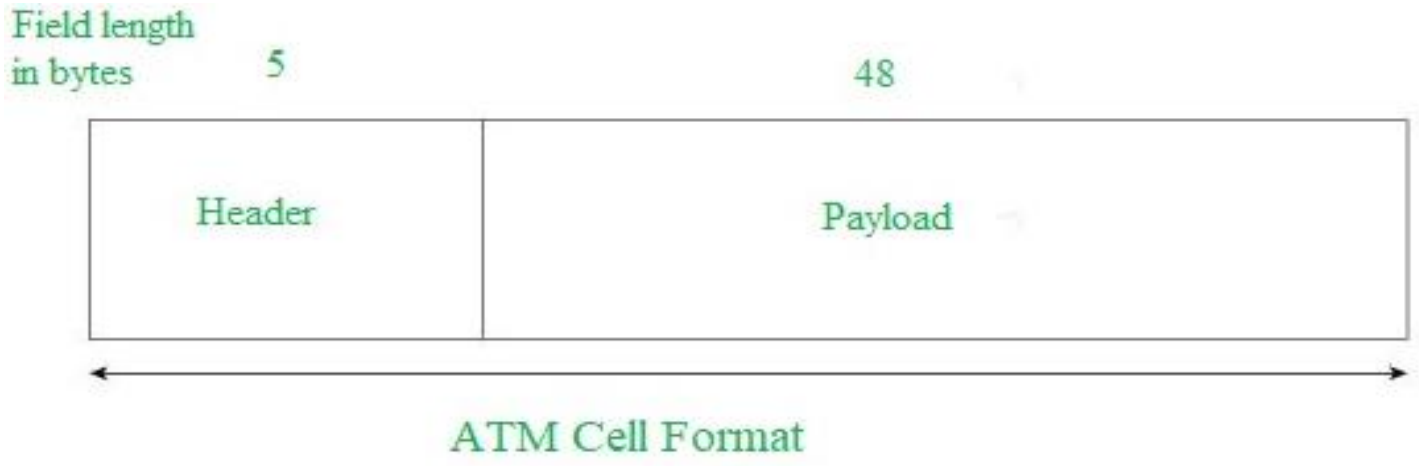
X.25, Frame Relay, ATM



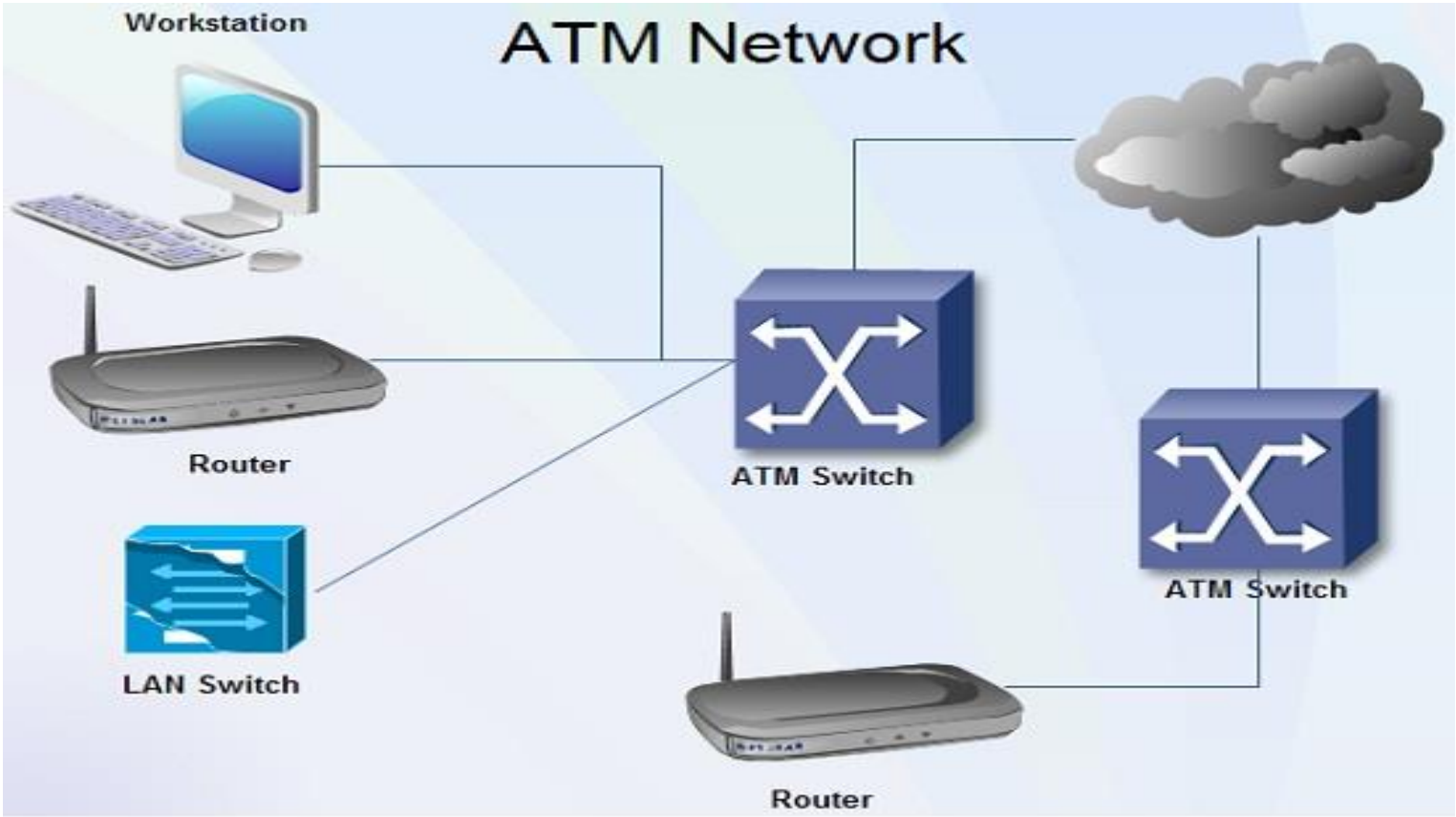
X.25, Frame Relay, ATM

- **Asynchronous Transfer Mode (ATM)**
- Asynchronous transfer mode (ATM), also known as cell relay, is similar in concept to frame relay.
- ATM is even more streamlined than frame relay in its functionality, and can support data rates several orders of magnitude greater than frame relay.
- The “asynchronous” in ATM means ATM devices do not send and receive information at fixed speeds or using a timer, but instead negotiate transmission speeds based on hardware and information flow reliability.
- The “transfer mode” in ATM refers to the fixed-size cell structure used for packaging information.
- ATM transfers information in fixed-size units called cells.
- Each cell consists of 53 octets, or bytes.

X.25, Frame Relay, ATM



X.25, Frame Relay, ATM



THANK YOU