GRAPHIC ERA HILL UNIVERSITY BHIMTAL CAMPUS
CSE 6TH SESSION 2023-24
COMPUTER NETWORKS-1(TCS 604)
UNIT-1 NOTES

Computer networks and internet:

a **Network** could be a association of 1 or additional computers placed in associate surroundings, and also the **Internet** is that the relationship of computers connecting them from everywhere on the planet. The basic distinction between network and net is that the **Network** consists of pieces that area unit physically connected and may be used as a private computer yet on share data with one another. Conversely, the **Internet** could be a technology that links these little and huge networks with one another and builds a additional in depth network.

S.NO	Network	Internet
1.	Network is defined as the group of two or more computer systems.	Whereas internet is the interrelationship of a few networks.
2.	The coverage of network is limited in comparison of internet.	While it covers large geographical area.
3.	It provides the link between many computers and network-enabled devices.	While it provide connection among many networks.
4.	The types of network are: LAN, MAN, WAN, CAN and HAN.	Whereas the types of internet is world wide web.
5.	Through network, hundreds or a few thousands of computer system can linked simultaneously.	While through internet, millions of computer system can linked simultaneously.
6.	It requires less number of hardware devices.	While it requires various hardware devices.

Network protocol:

In most cases, communication across a network like the Internet uses the OSI model. The OSI model has a total of seven layers. Secured connections, network management, and network communication are the three main tasks that the network protocol performs. The purpose of protocols is to link different devices.
The protocols can be broadly classified into three major categories:

1. Network Communication
2. Network Management
3. Network Security

1. Network Communication

Communication protocols are really important for the functioning of a network. They are so crucial that it is not possible to have computer networks without them. These protocols formally set out the rules and formats through which data is transferred. These protocols handle syntax, semantics, error detection, synchronization, and authentication.

1. **HTTP:** It is a layer 7 protocol that is designed for transferring a hypertext between two or more systems. HTTP works on a client-server model, most of the data sharing over the web is done through using HTTP.
2. **TCP:** TCP layouts a reliable stream delivery by using sequenced acknowledgment. It is a connection-oriented protocol i.e., it establishes a connection between applications before sending any data. It is used for communicating over a network. It has many applications such as emails, FTP, streaming media, etc.
3. **UDP:** It is a connectionless protocol that lay-out a basic but unreliable message service. It adds no flow control, reliability, or error-recovery functions. UPD is functional in cases where reliability is not required. It is used when we want faster transmission, for multicasting and broadcasting connections, etc.

Network Management

These protocols assist in describing the procedures and policies that are used in monitoring, maintaining, and managing the computer network. These protocols also help in communicating these requirements across the network to ensure stable communication. Network management protocols can also be used for troubleshooting connections between a host and a client.

Examples of Network Management Protocols:

1. **ICMP:** It is a layer 3 protocol that is used by network devices to forward operational information and error messages. ICMP is used for reporting congestions, network errors, diagnostic purposes, and timeouts.
2. **SNMP:** It is a layer 7 protocol that is used for managing nodes on an IP network. There are three main components in the SNMP protocol i.e., SNMP agent, SNMP manager, and managed device. SNMP agent has the local knowledge of management details, it translates those details into a form that is compatible with the SNMP manager. The manager presents data acquired from SNMP agents, thus helping in monitoring network glitches, and network performance, and troubleshooting them.
3. **Gopher:** It is a type of file retrieval protocol that provides downloadable files with some description for easy management, retrieving, and searching of files. All the files are arranged on a remote computer in a stratified manner. Gopher is an old protocol and it is not much used nowadays.
4. **FTP:** FTP is a Client/server protocol that is used for moving files to or from a host computer, it allows users to download files, programs, web pages, and other things that are available on other services.
5. **POP3:** It is a protocol that a local mail client uses to get email messages from a remote email server over a TCP/IP connection. Email servers hosted by ISPs also use the POP3 protocol to hold and receive emails intended for their users. Eventually, these users will use email client software to look at their mailbox on the remote server and to download their emails. After the email client downloads the emails, they are generally deleted from the servers.
6. **Telnet:** It is a protocol that allows the user to connect to a remote computer program and to use it i.e., it is designed for remote connectivity. Telnet creates a connection between a host machine and a remote endpoint to enable a remote session.

3. Network Security

These protocols secure the data in passage over a network. These protocols also determine how the network secures data from any unauthorized attempts to extract or review data. These protocols make sure that no unauthorized devices, users, or services can access the network data. Primarily, these protocols depend on encryption to secure data.

Examples of Network Security Protocols:

1. **SSL:** It is a network security protocol mainly used for protecting sensitive data and securing internet connections. SSL allows both server-to-server and client-to-server communication. All the data transferred through SSL is encrypted thus stopping any unauthorized person from accessing it.

2. **HTTPS:** It is the secured version of HTTP. this protocol ensures secure communication between two computers where one sends the request through the browser and the other fetches the data from the web server.
3. **TLS:** It is a security protocol designed for data security and privacy over the internet, its functionality is encryption, checking the integrity of data i.e., whether it has been tampered with or not, and authentication. It is generally used for encrypted communication between servers and web apps, like a web browser loading a website, it can also be used for encryption of messages, emails, and VoIP.

Access network and physical media:

An **access network** is a type of network which physically connects an end system to the immediate router (also known as the "edge router") on a path from the end system to any other distant end system. Examples of access networks are ISP, home networks, enterprise networks, ADSL, mobile network, FTTH etc.

Working Principle: At first, Before they may connect to an ISP, they must have a modem, router, or switch. Through a variety of network protocols, this device connects to the ISP's server and activates the connection. Users can select from a range of connection technologies, such as DSL, Ethernet, Wi-Fi, or 5G, depending on their location and type of equipment also.
The data is delivered across numerous linked devices in an access network using internal routing protocols like Internet Protocol (IP). This eliminates the need for external switches or routers by enabling direct communication between all devices connected to the same network.

Types of access networks:

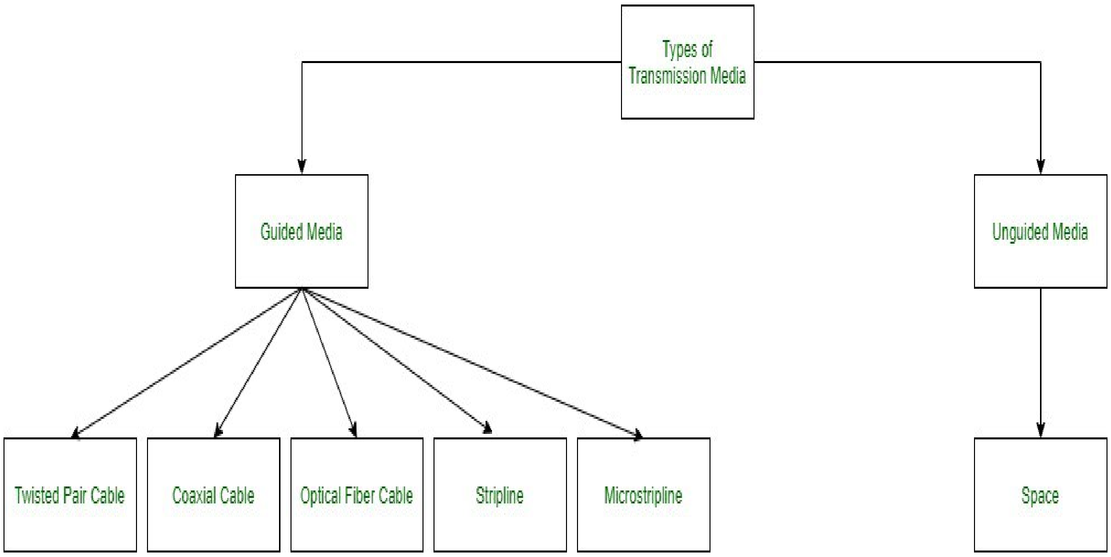
- **Ethernet –** It is the most commonly installed wired LAN technology and it provides services on the Physical and Data Link Layer of OSI reference model. Ethernet LAN typically uses coaxial cable or twisted pair wires.
- **DSL –** DSL stands for Digital Subscriber Line and DSL brings a connection into your home through telephone lines and a DSL line can carry both data and voice signals and the data part of the line is continuously connected. In DSL you are able to use the Internet and make phone calls simultaneously. **DSL** modem uses the telephone lines to exchange data with digital subscriber line access multiplexer (DSLAMs). In DSL we get **24 Mbps** downstream and **2.5 Mbps** upstream.
- **FTTH –** Fiber to the home (FTTH) uses optical fiber from a central Office (CO) directly to individual buildings and it provides high-speed Internet access among all access networks.It ensures high initial investment but

lesser future investment and it is the most expensive and most future-proof option amongst all these access networks.
- **Wireless LANs –** It links two or more devices using wireless communication within a range. It uses high-frequency radio waves and often include an access point for connecting to the Internet.

Types of Transmission Media

[redacted]

In data communication terminology, a transmission medium is a physical path between the transmitter and the receiver i.e. it is the channel through which data is sent from one place to another. Transmission Media is broadly classified into the following types:



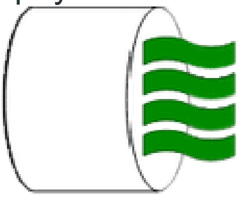
1. Guided Media: It is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links.
Features:
- High Speed
- Secure
- Used for comparatively shorter distances

There are 3 major types of Guided Media:

(i) Twisted Pair Cable –

It consists of 2 separately insulated conductor wires wound about each other. Generally, several such pairs are bundled together in a protective sheath. They are the most widely used Transmission Media. Twisted Pair is of two types:

- **Unshielded Twisted Pair (UTP):**
  UTP consists of two insulated copper wires twisted around one another. This type of cable has the ability to block interference and does not depend on a physical shield for this purpose. It is used for telephonic applications.



Unshielded Twisted Pair

Advantages:
⇢ Least expensive

⇢ Easy to install

⇢ High-speed capacity

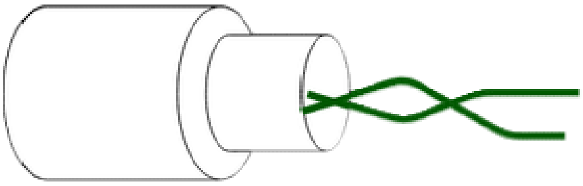
Disadvantages:
⇢ Susceptible to external interference

⇢ Lower capacity and performance in comparison to STP

⇢ Short distance transmission due to attenuation

Applications:
Used in telephone connections and LAN networks

- **Shielded Twisted Pair (STP):**
  This type of cable consists of a special jacket (a copper braid covering or a foil shield) to block external interference. It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.



Shielded Twisted Pair

Advantages:

⇢ Better performance at a higher data rate in comparison to UTP

⇢ Eliminates crosstalk

⇢ Comparatively faster

Disadvantages:

⇢ Comparatively difficult to install and manufacture

⇢ More expensive

⇢ Bulky

Applications:

The shielded twisted pair type of cable is most frequently used in extremely cold climates, where the additional layer of outer covering makes it perfect for withstanding such temperatures or for shielding the interior components.

(ii) Coaxial Cable –

It has an outer plastic covering containing an insulation layer made of PVC or Teflon and 2 parallel conductors each having a separate insulated protection cover. The coaxial cable transmits information in two modes: Baseband mode(dedicated cable bandwidth) and Broadband mode(cable bandwidth is split into separate ranges). Cable TVs and analog television networks widely use Coaxial cables.

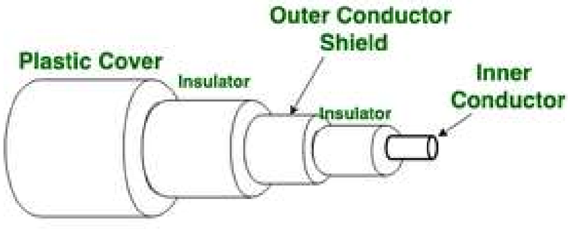


Figure of Coaxial Cable

Advantages:

- High Bandwidth
- Better noise Immunity
- Easy to install and expand
- Inexpensive

Disadvantages:

- Single cable failure can disrupt the entire network

Applications:

Radio frequency signals are sent over coaxial wire. It can be used for cable television signal distribution, digital audio (S/PDIF), computer network connections (like Ethernet), and feedlines that connect radio transmitters and receivers to their antennas.

(iii) Optical Fiber Cable –

It uses the concept of refraction of light through a core made up of glass or plastic. The core is surrounded by a less dense glass or plastic covering called the cladding. It is used for the transmission of large volumes of data.
The cable can be unidirectional or bidirectional. The WDM (Wavelength Division Multiplexer) supports two modes, namely unidirectional and bidirectional mode.

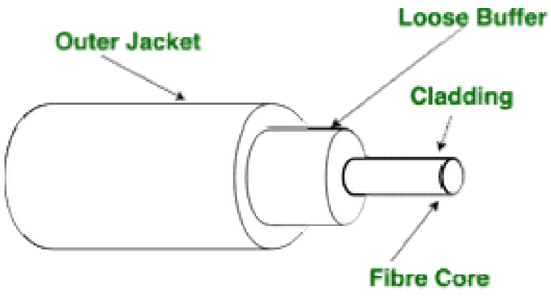


Figure of Optical Fibre Cable

Advantages:

- Increased capacity and bandwidth
- Lightweight
- Less signal attenuation
- Immunity to electromagnetic interference
- Resistance to corrosive materials

Disadvantages:

- Difficult to install and maintain
- High cost
- Fragile

Applications:

- Medical Purpose: Used in several types of medical instruments.
- Defence Purpose: Used in transmission of data in aerospace.
- For Communication: This is largely used in formation of internet cables.
- Industrial Purpose: Used for lighting purposes and safety measures in designing the interior and exterior of automobiles.

(iv) Stripline

Stripline is a transverse electromagnetic (TEM) transmission line medium invented by Robert M. Barrett of the Air Force Cambridge Research Centre in the 1950s. Stripline is the earliest form of the planar transmission line. It uses a conducting material to transmit high-frequency waves it is also called a waveguide. This conducting material is sandwiched between two layers of the ground plane which are usually shorted to provide EMI immunity.

(v) Microstripline
In this, the conducting material is separated from the ground plane by a layer of dielectric.

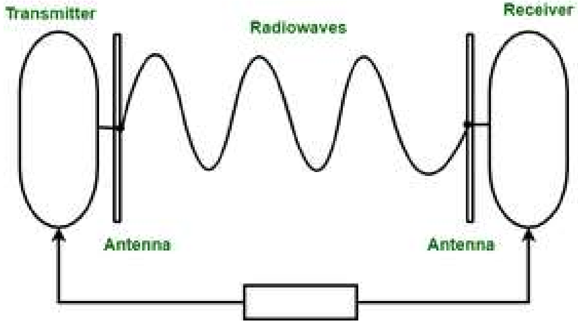
2. Unguided Media:
It is also referred to as Wireless or Unbounded transmission media. No physical medium is required for the transmission of electromagnetic signals.

Features:

- The signal is broadcasted through air
- Less Secure
- Used for larger distances

There are 3 types of Signals transmitted through unguided media:

(i) Radio waves –
These are easy to generate and can penetrate through buildings. The sending and receiving antennas need not be aligned. Frequency Range:3KHz – 1GHz. AM and FM radios and cordless phones use Radio waves for transmission.



Further Categorized as (i) Terrestrial and (ii) Satellite.

(ii) Microwaves –
It is a line of sight transmission i.e. the sending and receiving antennas need to be properly aligned with each other. The distance covered by the signal is directly proportional to the height of the antenna. Frequency Range:1GHz – 300GHz. These are majorly used for mobile phone communication and television distribution.

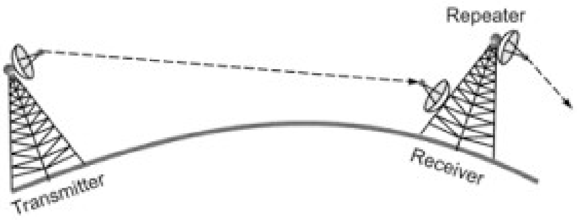


Fig: Microwave Transmission

Microwave Transmission

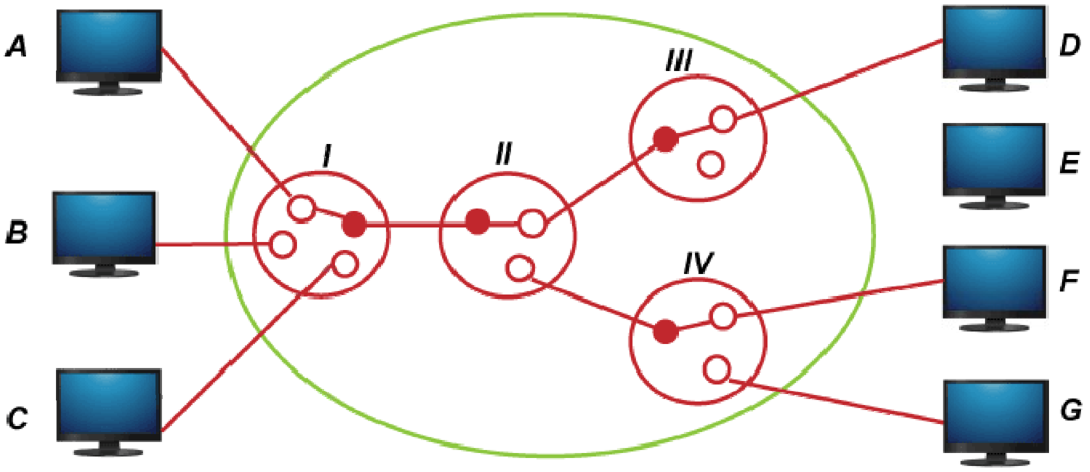
(iii) Infrared –
Infrared waves are used for very short distance communication. They cannot penetrate through obstacles. This prevents interference between systems. Frequency Range:300GHz – 400THz. It is used in TV remotes, wireless mouse, keyboard, printer, etc.

Circuit and packet switching:

Circuit switching Network:

A circuit-switched network is one of the simplest data communication methods in which a dedicated path is established between the sending and receiving device. In this physical links connect via a set of switches.

Following figure displays the working of circuit switched network.

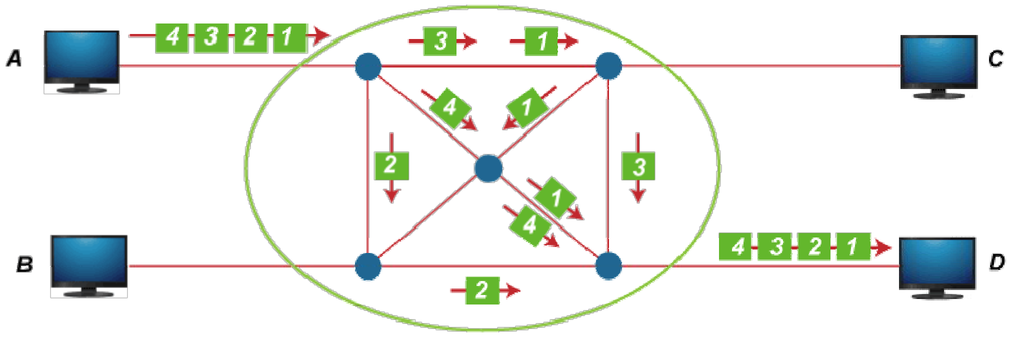


Circuit Switched Network

Packet switching Network:

In the Packet switching Network, the message is divide into packets. Each packet contains a header which includes the source address, destination address, and control information.

Following figure displays the working of packet switched network.



Packet Switched Network

In the above figure, it shows how a data gram approach is used to deliver four packets from station A to station D.

Following are the differences between circuit switching and packet switching networks.

S.No	Parameter	Circuit switching Network	Packet switching Network
1	Path	In circuit switched network a dedicated path is created between two points by setting the switches.	In packet switched network no dedicated path is created between two points. Only the virtual circuit exists.
2	Store and forward transmission	In circuit switching there is no concept of store and forward transmission.	In virtual packet switched network, each node may store incoming packets and forward them after use.
3	Dedicated	The links that make a path in circuit switched network are dedicated and cannot be used for other connections.	In the virtual circuit network, links that make a route can be dedicated with other connections.
4	Availability of Bandwidth	In circuit switching, bandwidth is fixed because it is reserved in advance.	In the virtual circuit network, require bandwidth is dynamic because it can be released as it is needed.
5	The route followed by packets	The route followed by packets is always the same.	The route followed by packets is may or may not be different.
6	Call setup	An in-circuit switching call setup is required.	In packet switching, call setup is not required.
7	Congestion	In circuit switching, congestion can occur at set up time.	In packet switching, congestion can occur on every packet.

8	Wastage of Bandwidth	In circuit switching, bandwidth is fixed, unused bandwidth on an allocated circuit is wasted.	Other packets from an unrelated source may utilize unused bandwidth.
9	Charging	In circuit switching, users are charged based on time and the basis of distance.	In packet switching, users are charged based on time and number of bytes carried & not based on distance.
10	Application	Telephone network for bidirectional, real time transfer of voice signal.	Internet for datagram and reliable stream service between computers.
11	Layers	Circuit-switched network is implemented at the physical layer.	A virtual circuit network is implemented at the data link and a network layer.
12	Reliability	Circuit-switched is highly reliable.	In packet switching, low reliability, subject to congestion.
13	Overhead bits	In Circuit-switched network, no overhead bits after call setup.	In packet switching, Overhead bits in each packet.
14	Technologies or types	Circuit switching using two technologies ○ Time Division Switching ○ Space Division Switching	Packet Switching using two technologies ○ Datagram circuit approach ○ Virtual circuit Approach
15	Installation Cost	Circuit switching's initial cost is low.	Packet switching networks have high installation costs.
16	Protocols	Circuit switching requires simple protocols for delivery.	Packet switching requires complex protocols for delivery.
17	Addressing scheme	In Circuit switching, Hierarchical numbering plan scheme is used.	In Packet switching, Hierarchical address space is

			used.
18	End Terminal	In this telephone and modem is used as end terminal.	In this computer is used as end terminal.
19	Information type	In this information type is Analog voice or PCM digital voices.	In this information type is binary information.
20	Multiplexing scheme	In circuit switching, circuit multiplexing is used.	In packet switching, packet multiplexing shared media access network in used.
21	Routing Scheme	In circuit switching, route selecting during set up.	In packet switching, each packet is routed independently.

Internet backbone:

Backbone LANs:

Because of increasing use of distributed applications and PCs, a new flexible strategy for LANs has been introduced. if a premises wide data communication system is to be supported then we need a networking system which can span over the required distance and which capable of interconnecting all the equipment in a single building or in a group of buildings.

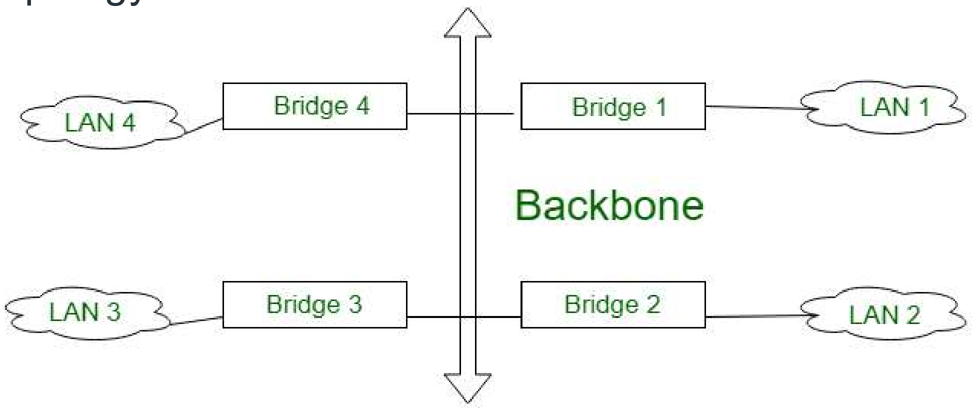
It is possible to develop a single LAN for this purpose but practically this scheme faces the following drawbacks:

1. **Poor Reliability:**
   With a single LAN, the reliability will be poor since a service interruption even for a short duration can cause major problem to the user.
2. **Capacity:**
   There is a possibility that a single LAN may be saturated due to increase in number of devices beyond a certain number

3. **Cost:**
   A single LAN can not give its optimum performance for the diverse requirements of communication and interconnection.

So the alternative for using a single LAN is to use low cost low capacity LANs in each building or department and then interconnection all these LANs with high capacity LAN. such a network is called as **Backbone LAN**. the backbone network allows several LANs to be connected. in the backbone network, no station is directly connected with backbone, instead each station is a part of a LAN, and the LANs are connected to the backbone.
The backbone itself is a LAN, it uses a LAN protocol such as ethernet, Hence each connection in the backbone is itself another LAN. The two very common used architectures are: Bus backbone, Star backbone. These are explained as following below.

1. **Bus Backbone:**
   In Bus backbone the topology used for the backbone is bus topology.

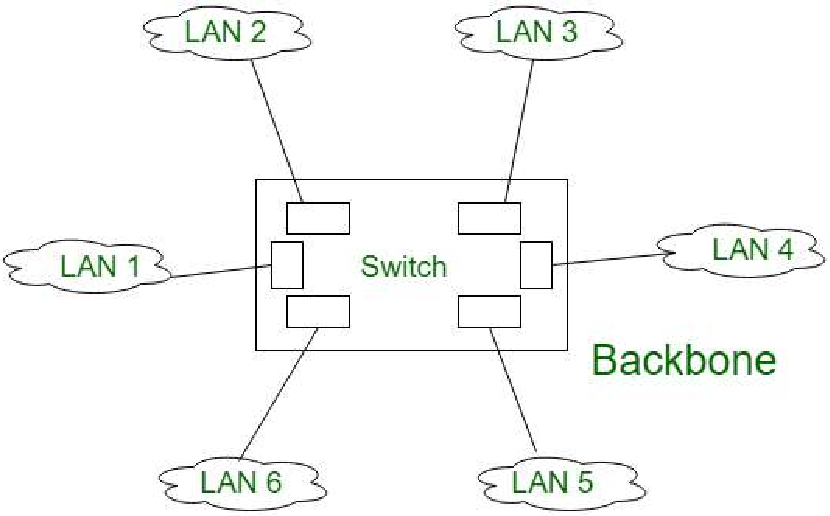


Structure of a Bus backbone

In above the Bus backbone structure is used as a distribution backbone for connecting different buildings in an organization. each building may have either a single LAN or another backbone which comes in star backbone. the structure is a bridge based (bridge is the connecting device) backbone with four LANs.

Working:
In above structure if a station in LAN 2 wants to send a frame to some other station in Same LAN then Bridge 2 will not allow the frame to pass to any other LAN, hence this frame will not reach the backbone. If a station from LAN 1 wants to send a frame to a station in LAN 4 then Bridge 1 passes this frame to the backbone. This frame is then received by Bridge 4 and delivered to the destination.

2. **Star Backbone:**
   The topology of this backbone is star topology.

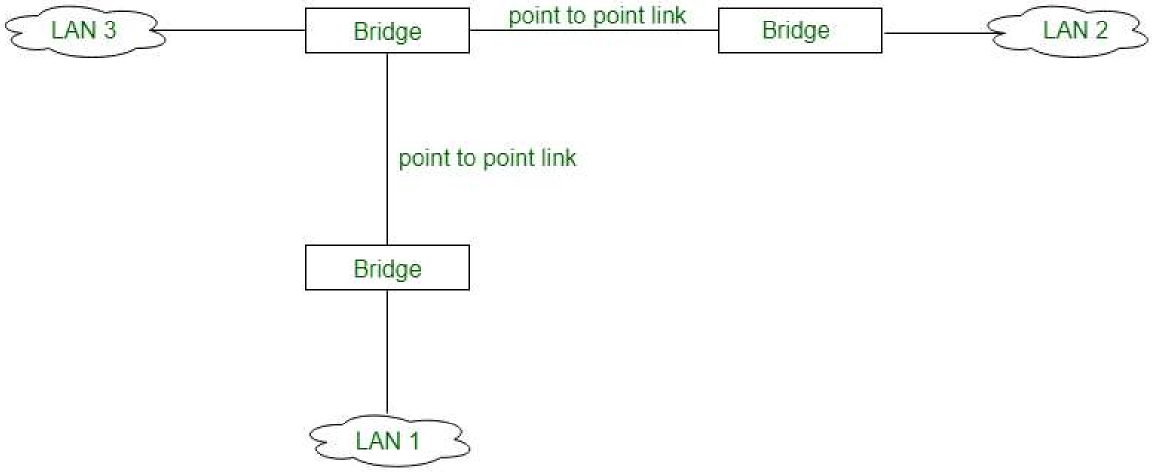


Star Backbone

Above figure shows the Star backbone in this configuration, the backbone is simply a switch which is used to connect various LANs. The switch does the job of backbone and connect the LANs as well. This type of backbone are basically used as distribution backbone inside a building.

There is one more category of backbone network is Interconnecting of Remote LANs:

3. **Interconnection of Remote control:**
   In this type of backbone network the connection are done through the bridge called remote bridges which acts as connecting devices in connect LANs as point to point network link.



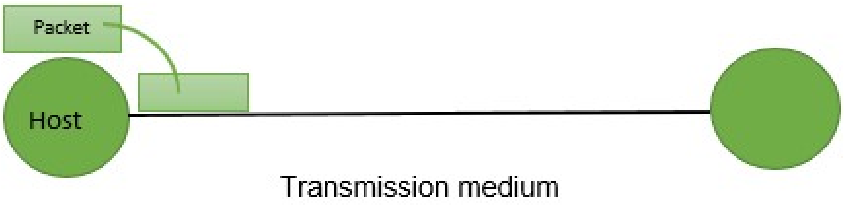
Connecting remote LANs to each other

Example of point to point networks are leased telephone lines or ADLS lines. Such a point to point network can be considered as being equivalent ta a LAN without stations.

TYPES OF DELAYS:

The delays, here, means the time for which the processing of a particular packet takes place. We have the following types of delays in computer networks:

1. Transmission Delay:
The time taken to transmit a packet from the host to the transmission medium is called Transmission delay.



For example, if bandwidth is 1 bps (every second 1 bit can be transmitted onto the transmission medium) and data size is 20 bits then what is the transmission delay? If in one second, 1 bit can be transmitted. To transmit 20 bits, 20 seconds would be required.

Let B bps is the bandwidth and L bit is the size of the data then transmission delay is,

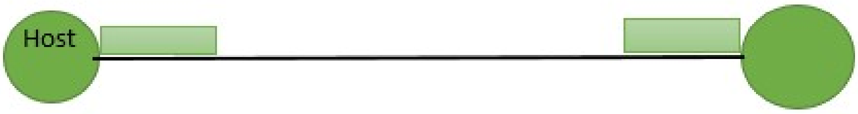
```
Tt = L/B
```

This delay depends upon the following factors:

- If there are multiple active sessions, the delay will become significant.
- Increasing bandwidth decreases transmission delay.
- MAC protocol largely influences the delay if the link is shared among multiple devices.
- Sending and receiving a packet involves a context switch in the operating system, which takes a finite time.

2. Propagation delay:

After the packet is transmitted to the transmission medium, it has to go through the medium to reach the destination. Hence the time taken by the last bit of the packet to reach the destination is called propagation delay.



Factors affecting propagation delay:

1. **Distance –** It takes more time to reach the destination if the distance of the medium is longer.
2. **Velocity –** If the velocity(speed) of the medium is higher, the packet will be received faster.

```
Tp = Distance / Velocity
```

Note:

```
Velocity =3 X 10^8 m/s (for air)

Velocity= 2.1 X 10^8 m/s (for optical fibre)
```

3. Queueing delay:
Let the packet is received by the destination, the packet will not be processed by the destination immediately. It has to wait in a queue in something called a buffer. So the amount of time it waits in queue before being processed is called queueing delay. In general, we can’t calculate queueing delay because we don’t have any formula for that.

This delay depends upon the following factors:

- If the size of the queue is large, the queuing delay will be huge. If the queue is empty there will be less or no delay.
- If more packets are arriving in a short or no time interval, queuing delay will be large.
- The less the number of servers/links, the greater is the queuing delay.

4. Processing delay:

Now the packet will be taken for the processing which is called processing delay.
Time is taken to process the data packet by the processor that is the time required by intermediate routers to decide where to forward the packet, update TTL, perform header checksum calculations.

It also doesn’t have any formula since it depends upon the speed of the processor and the speed of the processor varies from computer to computer.

Note: Both queueing delay and processing delay doesn’t have any formula because they depend on the speed of the processor
This delay depends upon the following factors:

- It depends on the speed of the processor.

```
Ttotal = Tt + Tp + Tq + Tpro


Ttotal = Tt+Tp

(when taking Tq and Tpro equals to 0)
```

The LAYERD ARCHITECTURE:

Protocol layering:

A communication subsystem is a complex piece of Hardware and software. Early attempts for implementing the software for such subsystems were based on a single, complex, unstructured program with many interacting components. The resultant software was very difficult to test and modify. To overcome such problem, the ISO has developed a layered approach. In a layered approach, networking concept is divided into several layers, and each layer is assigned a particular task. Therefore, we can say that networking tasks depend upon the layers.

Layered Architecture

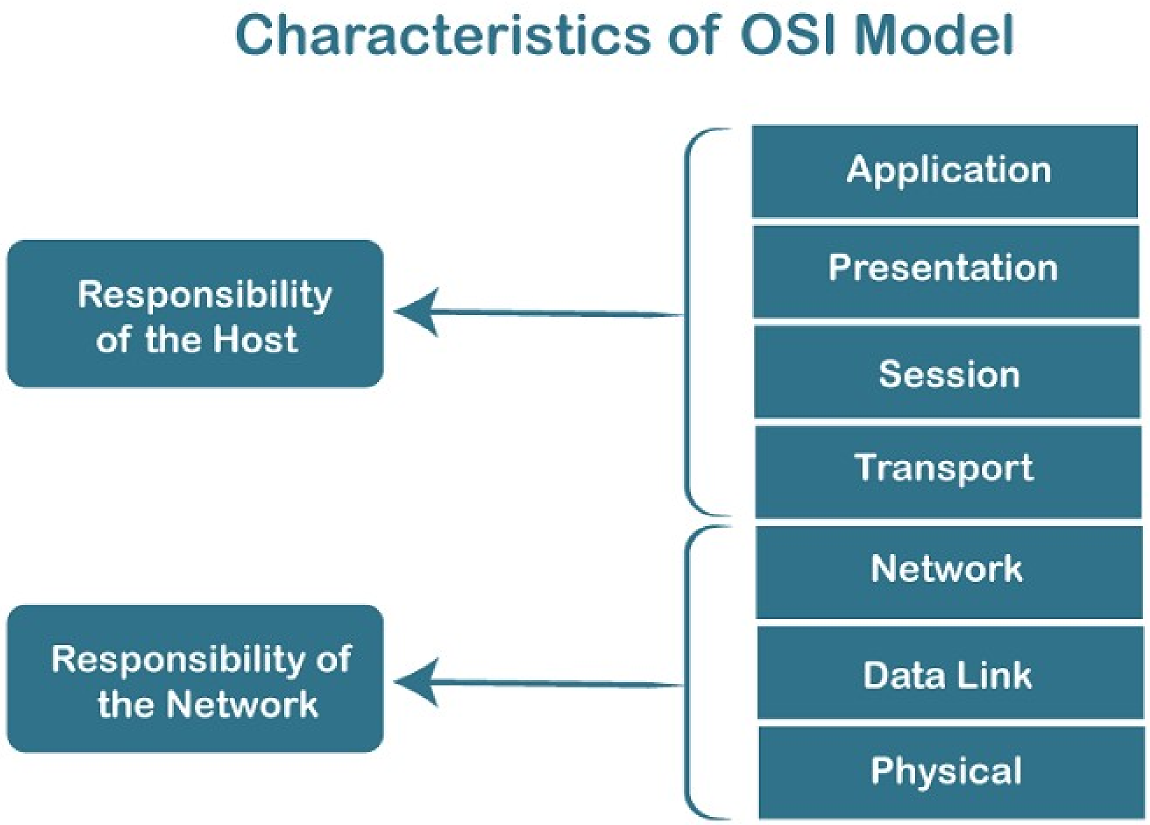
- The main aim of the layered architecture is to divide the design into small pieces.
- Each lower layer adds its services to the higher layer to provide a full set of services to manage communications and run the applications.
- It provides modularity and clear interfaces, i.e., provides interaction between subsystems.
- It ensures the independence between layers by providing the services from lower to higher layer without defining how the services are implemented. Therefore, any modification in a layer will not affect the other layers.
- The basic elements of layered architecture are services, protocols, and interfaces.
    - **Service:** It is a set of actions that a layer provides to the higher layer.
    - **Protocol:** It defines a set of rules that a layer uses to exchange the information with peer entity. These rules mainly concern about both the contents and order of the messages used.
    - **Interface:** It is a way through which the message is transferred from one layer to another layer.
- In a layer n architecture, layer n on one machine will have a communication with the layer n on another machine and the rules used in a conversation are known as a layer-n protocol.

- In case of layered architecture, no data is transferred from layer n of one machine to layer n of another machine. Instead, each layer passes the data to the layer immediately just below it, until the lowest layer is reached.
- Below layer 1 is the physical medium through which the actual communication takes place.
- In a layered architecture, unmanageable tasks are divided into several small and manageable tasks.
- The data is passed from the upper layer to lower layer through an interface. A Layered architecture provides a clean-cut interface so that minimum information is shared among different layers. It also ensures that the implementation of one layer can be easily replaced by another implementation.
- A set of layers and protocols is known as network architecture.

OSI Model

- OSI stands for **Open System Interconnection** is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
- OSI consists of seven layers, and each layer performs a particular network function.
- OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.
- OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.

Characteristics of OSI Model:


Characteristics of OSI Model
Responsibility of the Host
Responsibility of the Network
Application
Presentation
Session
Transport
Network
Data Link
Physical

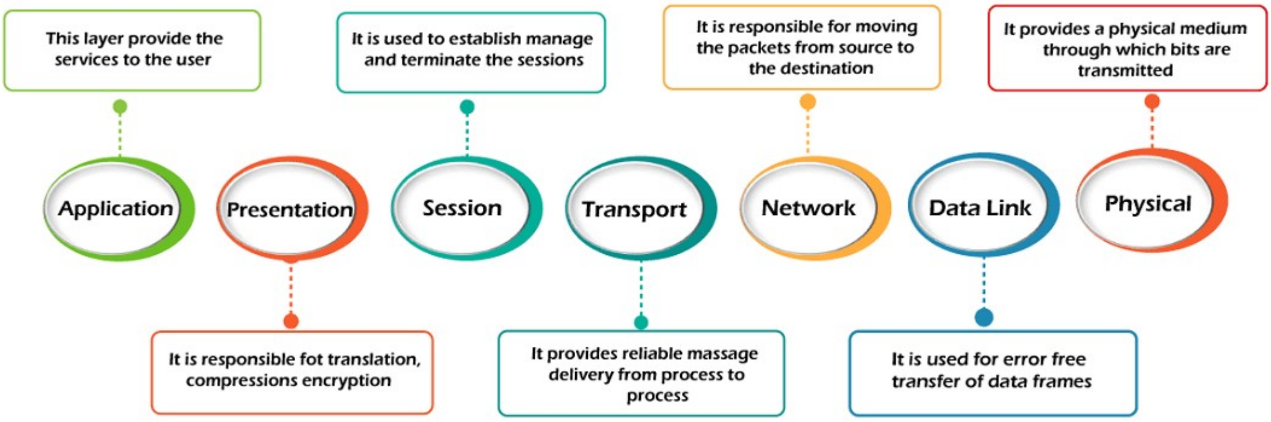
- The OSI model is divided into two layers: upper layers and lower layers.
- The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer interact with the software applications. An upper layer refers to the layer just above another layer.
- The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is the lowest layer of the OSI model and is closest to the physical medium. The

physical layer is mainly responsible for placing the information on the physical medium.

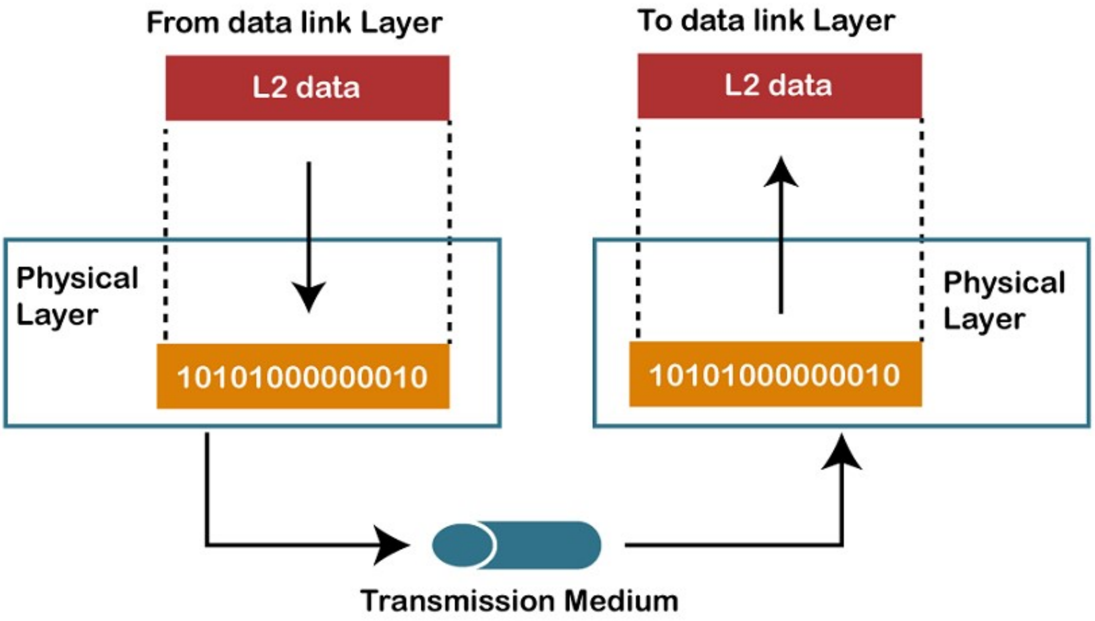
7 Layers of OSI Model

There are the seven OSI layers. Each layer has different functions. A list of seven layers are given below:

1. Physical Layer
2. Data-Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer


This layer provide the services to the user
It is used to establish manage and terminate the sessions
It is responsible for moving the packets from source to the destination
It provides a physical medium through which bits are transmitted
Application
Presentation
Session
Transport
Network
Data Link
Physical
It is responsible fot translation, compressions encryption
It provides reliable massage delivery from process to process
It is used for error free transfer of data frames

1) Physical layer

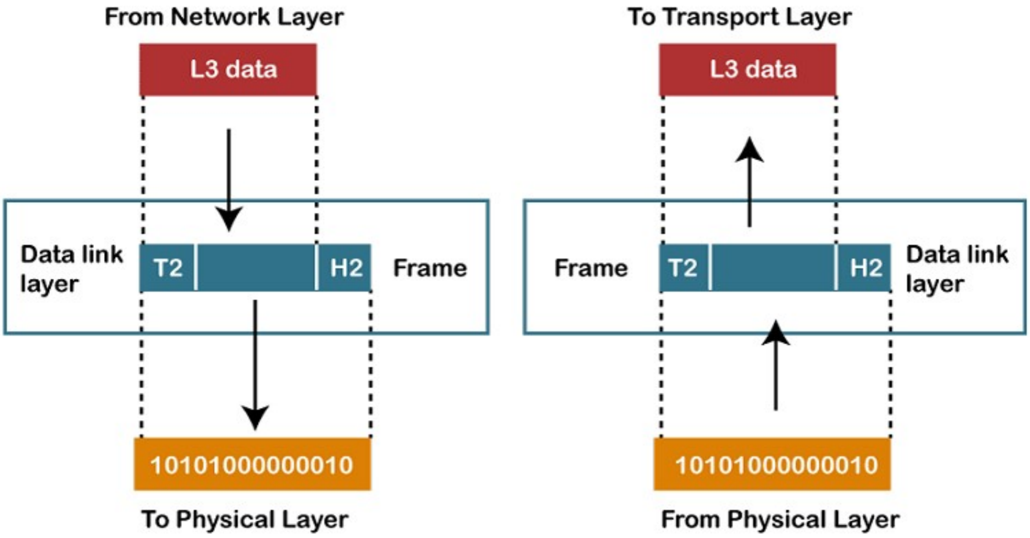


- The main functionality of the physical layer is to transmit the individual bits from one node to another node.
- It is the lowest layer of the OSI model.
- It establishes, maintains and deactivates the physical connection.
- It specifies the mechanical, electrical and procedural network interface specifications.

Functions of a Physical layer:

- **Line Configuration:** It defines the way how two or more devices can be connected physically.
- **Data Transmission:** It defines the transmission mode whether it is simplex, half-duplex or full-duplex mode between the two devices on the network.
- **Topology:** It defines the way how network devices are arranged.
- **Signals:** It determines the type of the signal used for transmitting the information.

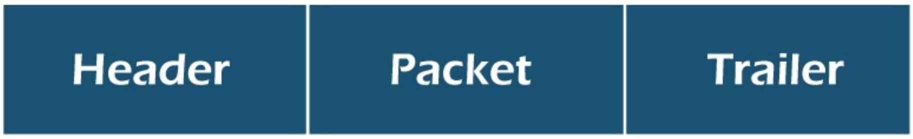
2) Data-Link Layer



- This layer is responsible for the error-free transfer of data frames.
- It defines the format of the data on the network.
- It provides a reliable and efficient communication between two or more devices.
- It is mainly responsible for the unique identification of each device that resides on a local network.
- It contains two sub-layers:
  - **Logical Link Control Layer**
    - It is responsible for transferring the packets to the Network layer of the receiver that is receiving.
    - It identifies the address of the network layer protocol from the header.
    - It also provides flow control.
  - **Media Access Control Layer**
    - A Media access control layer is a link between the Logical Link Control layer and the network's physical layer.
    - It is used for transferring the packets over the network.

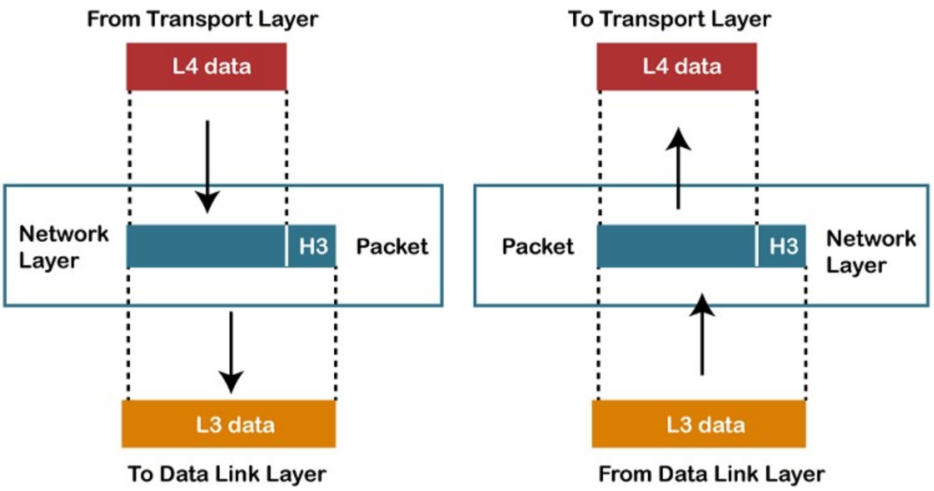
Functions of the Data-link layer

- **Framing:** The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame. The header which is added to the frame contains the hardware destination and source address.



- **Physical Addressing:** The Data link layer adds a header to the frame that contains a destination address. The frame is transmitted to the destination address mentioned in the header.
- **Flow Control:** Flow control is the main functionality of the Data-link layer. It is the technique through which the constant data rate is maintained on both the sides so that no data get corrupted. It ensures that the transmitting station such as a server with higher processing speed does not exceed the receiving station, with lower processing speed.
- **Error Control:** Error control is achieved by adding a calculated value CRC (Cyclic Redundancy Check) that is placed to the Data link layer's trailer which is added to the message frame before it is sent to the physical layer. If any error seems to occurr, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.
- **Access Control:** When two or more devices are connected to the same communication channel, then the data link layer protocols are used to determine which device has control over the link at a given time.

3) Network Layer



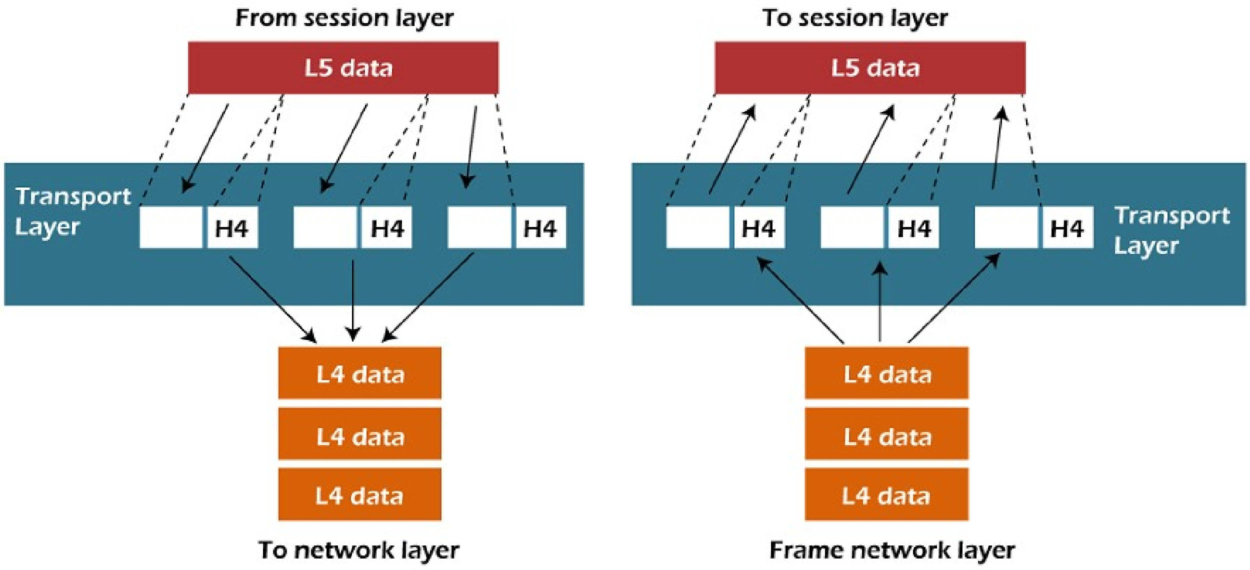
- It is a layer 3 that manages device addressing, tracks the location of devices on the network.
- It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
- The Data link layer is responsible for routing and forwarding the packets.
- Routers are the layer 3 devices, they are specified in this layer and used to provide the routing services within an internetwork.
- The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IP and Ipv6.

Functions of Network Layer:

- **Internetworking:** An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.
- **Addressing:** A Network layer adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet.

- **Routing:** Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.
- **Packetizing:** A Network Layer receives the packets from the upper layer and converts them into packets. This process is known as Packetizing. It is achieved by internet protocol (IP).

4) Transport Layer



- The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.
- The main responsibility of the transport layer is to transfer the data completely.
- It receives the data from the upper layer and converts them into smaller units known as segments.
- This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably.

The two protocols used in this layer are:

- **Transmission Control Protocol**
    - It is a standard protocol that allows the systems to communicate over the internet.
    - It establishes and maintains a connection between hosts.
    - When data is sent over the TCP connection, then the TCP protocol divides the data into smaller units known as segments. Each segment travels over the internet using multiple routes, and they arrive in different orders at the destination. The transmission control protocol reorders the packets in the correct order at the receiving end.
- **User Datagram Protocol**
    - User Datagram Protocol is a transport layer protocol.
    - It is an unreliable transport protocol as in this case receiver does not send any acknowledgment when the packet is received, the sender does not wait for any acknowledgment. Therefore, this makes a protocol unreliable.

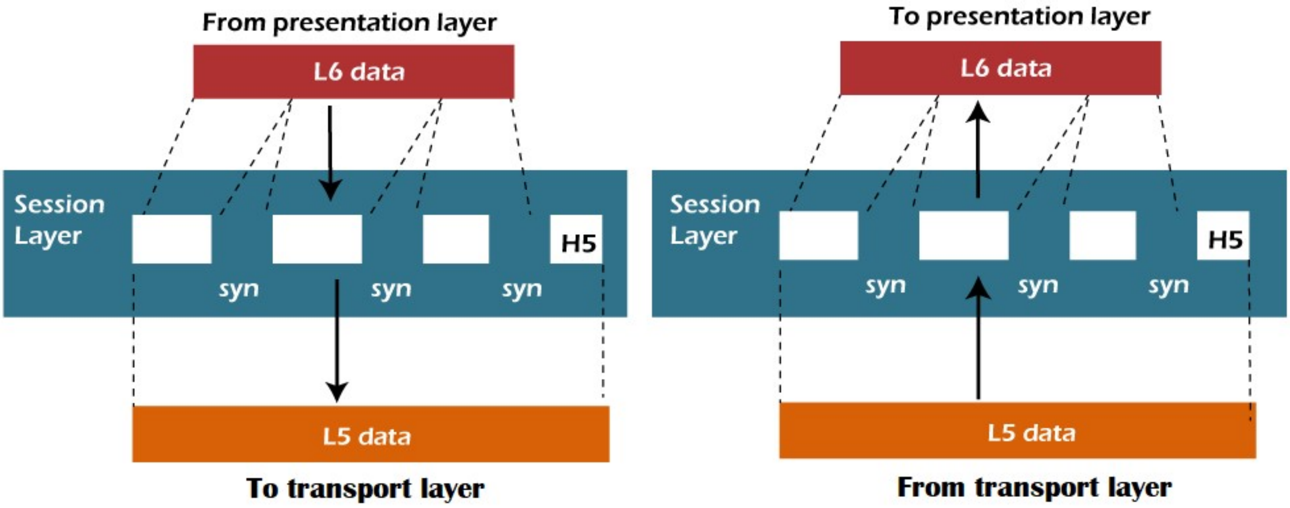
Functions of Transport Layer:

- **Service-point addressing:** Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the address known as a service-point address or port address. The responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.
- **Segmentation and reassembly:** When the transport layer receives the message from the upper layer, it divides the

message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.

- **Connection control:** Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.
- **Flow control:** The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.
- **Error control:** The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link. The sender transport layer ensures that message reach at the destination without any error.

5) Session Layer

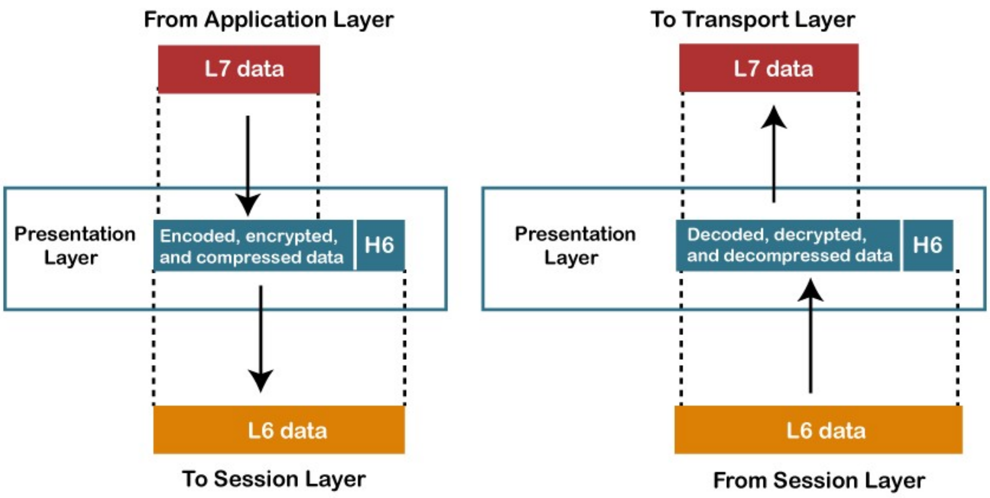


- It is a layer 3 in the OSI model.
- The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

Functions of Session layer:

- **Dialog control:** Session layer acts as a dialog controller that creates a dialog between two processes or we can say that it allows the communication between two processes which can be either half-duplex or full-duplex.
- **Synchronization:** Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint. This process is known as Synchronization and recovery.

6) Presentation Layer



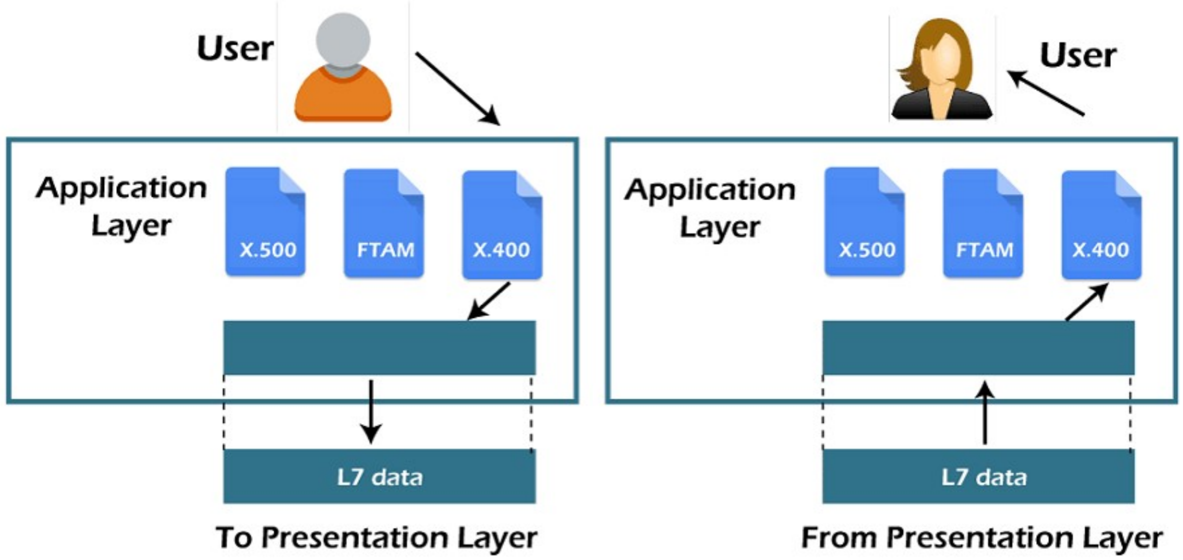
- A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.
- It acts as a data translator for a network.
- This layer is a part of the operating system that converts the data from one presentation format to another format.
- The Presentation layer is also known as the syntax layer.

Functions of Presentation layer:

- **Translation:** The processes in two systems exchange the information in the form of character strings, numbers and so on. Different computers use different encoding methods, the presentation layer handles the interoperability between the different encoding methods. It converts the data from sender-dependent format into a common format and changes the common format into receiver-dependent format at the receiving end.
- **Encryption:** Encryption is needed to maintain privacy. Encryption is a process of converting the sender-transmitted information into another form and sends the resulting message over the network.

- **Compression:** Data compression is a process of compressing the data, i.e., it reduces the number of bits to be transmitted. Data compression is very important in multimedia such as text, audio, video.

7) Application Layer



- An application layer serves as a window for users and application processes to access network service.
- It handles issues such as network transparency, resource allocation, etc.
- An application layer is not an application, but it performs the application layer functions.
- This layer provides the network services to the end-users.

Functions of Application layer:

- **File transfer, access, and management (FTAM):** An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.

- **Mail services:** An application layer provides the facility for email forwarding and storage.
- Directory services: An application provides the distributed database sources and is used to provide that global information about various objects.

TCP/IP MODEL:

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.

TCP/IP 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 the seven layers in the OSI model.

TCP and IP are different protocols of Computer Networks. The basic difference between TCP (Transmission Control Protocol) and IP (Internet Protocol) is in the transmission of data. In simple words, IP finds the destination of the mail and TCP has the work to send and receive the mail. UDP is another protocol, which does not require IP to communicate with another computer. IP is required by only TCP. This is the basic difference between TCP and IP.

Layers of TCP/IP Model

1. Application Layer
2. Transport Layer(TCP/UDP)

3. Network/Internet Layer(IP)
4. Data Link Layer (MAC)
5. Physical Layer

1. Physical Layer

It is a group of applications requiring network communications. This layer is responsible for generating the data and requesting connections. It acts on behalf of the sender and the Network Access layer on the behalf of the receiver. During this article, we will be talking on the behalf of the receiver.

2. Data Link Layer

The packet's network protocol type, in this case, TCP/IP, is identified by the data-link layer. Error prevention and "framing" are also provided by the data-link layer. Point-to-Point Protocol (PPP) framing and Ethernet IEEE 802.2 framing are two examples of data-link layer protocols.

3. Internet Layer

This layer parallels the functions of OSI's Network layer. It defines the protocols which are responsible for the logical transmission of data over the entire network. The main protocols residing at this layer are as follows:

- **IP:** IP stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions: IPv4 and IPv6. IPv4 is the one that most websites are using currently. But IPv6 is growing as the number of IPv4 addresses is limited in number when compared to the number of users.

- **ICMP:** ICMP stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
- **ARP:** ARP stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP, and Inverse ARP.

The Internet Layer is a layer in the Internet Protocol (IP) suite, which is the set of protocols that define the Internet. The Internet Layer is responsible for routing packets of data from one device to another across a network. It does this by assigning each device a unique IP address, which is used to identify the device and determine the route that packets should take to reach it.

4. Transport Layer

The TCP/IP transport layer protocols exchange data receipt acknowledgments and retransmit missing packets to ensure that packets arrive in order and without error. End-to-end communication is referred to as such. Transmission Control Protocol (TCP) and User Datagram Protocol are transport layer protocols at this level (UDP).

- **TCP:** Applications can interact with one another using TCP as though they were physically connected by a circuit. TCP transmits data in a way that resembles character-by-character transmission rather than separate packets. A starting point that establishes the connection, the whole transmission in byte order, and an ending point that closes the connection make up this transmission.
- **UDP:** The datagram delivery service is provided by UDP, the other transport layer protocol. Connections between receiving and sending hosts are not verified by UDP. Applications that transport little amounts of data use UDP rather than TCP because it eliminates the processes of establishing and validating connections.

5. Application Layer

This layer is analogous to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The three main protocols present in this layer are:

- **HTTP and HTTPS:** HTTP stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL(Secure Socket Layer). It is efficient in cases where the browser needs to fill out forms, sign in, authenticate, and carry out bank transactions.
- **SSH:** SSH stands for Secure Shell. It is a terminal emulations software similar to Telnet. The reason SSH is preferred is because of its ability to maintain the encrypted connection. It sets up a secure session over a TCP/IP connection.
- **NTP:** NTP stands for Network Time Protocol. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions. Assume the following situation without the presence of NTP. Suppose you carry out a transaction, where your computer reads the time at 2:30 PM while the server records it at 2:28 PM. The server can crash very badly if it's out of sync.

The host-to-host layer is a layer in the OSI (Open Systems Interconnection) model that is responsible for providing communication between hosts (computers or other devices) on a network. It is also known as the transport layer.

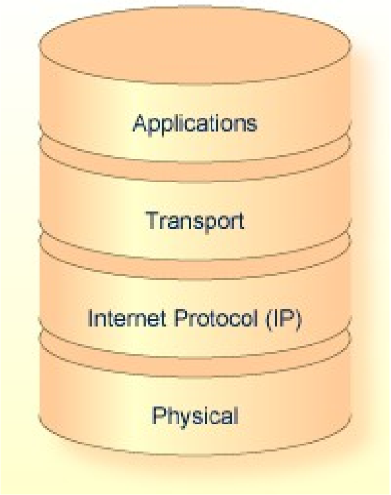
TCP/IP PROTOCOL STACK:

TCP/IP Protocol Stack

As shown in the following diagram, the TCP/IP protocol stack contains four layers:

- Physical layer
- Internet Protocol (IP) layer

- Transport layer, comprising
  - Transmission Control Protocol (TCP); and
  - User Datagram Protocol (UDP)
- Applications layer



Physical Layer

At the bottom of the stack is the physical layer, which deals with the actual transmission of data over physical media such as serial lines, Ethernet, token rings, FDDI rings, and hyperchannels. Messages can also be sent and received over other, non-physical access methods such as VTAM/SNA.

Internet Protocol (IP) Layer

Above the physical layer is the Internet Protocol (IP) layer, which deals with the routing of packets from one computer to another. The IP layer

- determines which lower level protocol to use when multiple interfaces exist.
- determines whether to send a packet directly to the host or indirectly to a relay host known as a router.
  When a packet is larger than the size supported by the physical medium, the IP layer breaks the packet into smaller packets, a process referred to as "fragmentation and reassembly".
- provides some control services for packets, and ensures that they are not sent from router to router indefinitely.

However, the IP layer does not keep track of a packet after it is sent, nor does it guarantee that the packet will be delivered.

Transport Layer

Above the IP layer is the transport layer, which contains the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP).

Transmission Control Protocol (TCP)

The Transmission Control Protocol (TCP) guarantees that data sent by higher levels is delivered in order and without corruption. To accomplish this level of service, the TCP implementation on one computer establishes a session or connection with the TCP implementation on another computer. This process is referred to as Connection Oriented Transport Service (COTS).

After a session is established, data is sent and received as a stream of contiguous bytes; each byte can be referenced by an exact sequence number. When data is received by the remote TCP, it sends an acknowledgment back to the local TCP advising it of the sequence number of the last byte of data received. If an acknowledgment is not received, or if an acknowledgment for previously sent data is received twice, the local TCP retransmits the data until it is all acknowledged. The remote TCP discards any bytes that are received more than once.

All data sent and received by TCP is validated for corruption using checksums. Whenever a checksum is incorrect, the bad data is discarded by TCP, and the correct data is retransmitted until it is accurately received.

User Datagram Protocol (UDP)

Unlike the TCP, the User Datagram Protocol (UDP) transmits and receives data in packets (datagrams), and delivery is not guaranteed. The contents of the data can be sent with or without a checksum. The use of checksums varies widely from one implementation to another.

Applications Layer

Above the transport layer is the applications layer, which contains both general applications and function libraries for use by applications.

Some general applications that run over TCP include

- File Transfer Protocol (FTP);
- remote terminal emulation (TELNET in line mode, TN3270 in full screen);
- Electronic Mail (SMTP); and
- Entire Net-Work.
  Some general applications that run over UDP are

- Network File Server (NFS); and
- Domain Name Server (DNS).