CST 303 Computer Networks

Vipin Das
Dept.of CSE

What we will learn?

- **The basic concepts of networking.**
- **The concepts behind desigining a network.**
- **Various protocols associated with networks.**
- **Common devices and features.**
- **The principle behind the transmission of the data.**

Impact of the subject.

- The subject knowledge is widely quizzed in almost all interviews and viva.
- The subject contents are more or less same across the globe.
- Many application domains require knowledge about the key concepts.

Text Books

1. Andrew S. Tanenbaum, Computer Networks, 4/e, PHI (Prentice Hall India).

2. Behrouz A Forouzan, Data Communication and Networking, 4/e, Tata McGraw Hill

Syllabus

Module - 1 (Introduction and Physical Layer)

Introduction – Uses of computer networks, Network hardware, Network software. Reference models – The OSI reference model, The TCP/IP reference model, Comparison of OSI and TCP/IP reference models.

Physical Layer – Modes of communication, Physical topologies, Signal encoding, Repeaters and hub, Transmission media overview. Performance indicators – Bandwidth, Throughput, Latency, Queuing time, Bandwidth–Delay product.

Module - 2 (Data Link Layer)

Data link layer - Data link layer design issues, Error detection and correction, Sliding window protocols, High-Level Data Link Control(HDLC)protocol. Medium Access Control (MAC) sublayer –Channel allocation problem, Multiple access protocols, Ethernet, Wireless LANs - 802.11, Bridges & switches - Bridges from 802.x to 802.y, Repeaters, Hubs, Bridges, Switches, Routers and Gateways.

Module - 3 (Network Layer)

Network layer design issues. Routing algorithms - The Optimality Principle, Shortest path routing, Flooding, Distance Vector Routing, Link State Routing, Multicast routing, Routing for mobile hosts. Congestion control algorithms. Quality of Service (QoS) - requirements, Techniques for achieving good QoS.

Module - 4 (Network Layer in the Internet)

IP protocol, IP addresses, Internet Control Message Protocol (ICMP), Address Resolution Protocol (ARP), Reverse Address Resolution Protocol (RARP), Bootstrap Protocol (BOOTP), Dynamic Host Configuration Protocol (DHCP). Open Shortest Path First(OSPF) Protocol, Border Gateway Protocol (BGP), Internet multicasting, IPv6, ICMPv6.

Module – 5 (Transport Layer and Application Layer)

Transport service – Services provided to the upper layers, Transport service primitives. User Datagram Protocol (UDP). Transmission Control Protocol (TCP) – Overview of TCP, TCP segment header, Connection establishment &release, Connection management modeling, TCP retransmission policy, TCP congestion control.

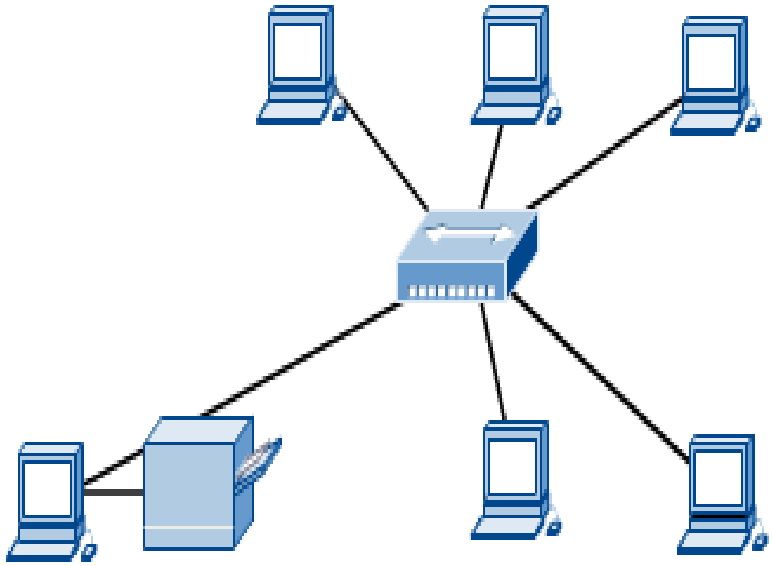
Application Layer –File Transfer Protocol (FTP), Domain Name System (DNS), Electronic mail, Multipurpose Internet Mail Extension (MIME), Simple Network Management Protocol

(SNMP), World Wide Web(WWW) – Architectural overview.

Module 1

What are computer networks ?

- **Computer network connects two or more autonomous computers / peripherals.**
- **The computers can be geographically located anywhere.**



Applications

Resource Sharing

- Hardware (computing resources, disks, printers)
- Software (application software)

Information Sharing

- Easy accessibility from anywhere (files, databases)
- Search Capability (WWW)

Communication

- Email
- Message broadcast

Remote computing

Distributed processing ***Ex:- Cloud Computing***

LAN,MAN & WAN

- **Network in small geographical Area (Room, Building or a Campus) is called LAN (Local Area Network)**
- **Network in a City is call MAN (Metropolitan Area Network)**
- **Network spread geographically (Country or across Globe) is called WAN (Wide Area Network)**

Ref :- Andrew S Tanenbaum 4/e

LAN

- A network of computers that are in the same physical location, such as home or building
- Usually connected using Ethernet standard.

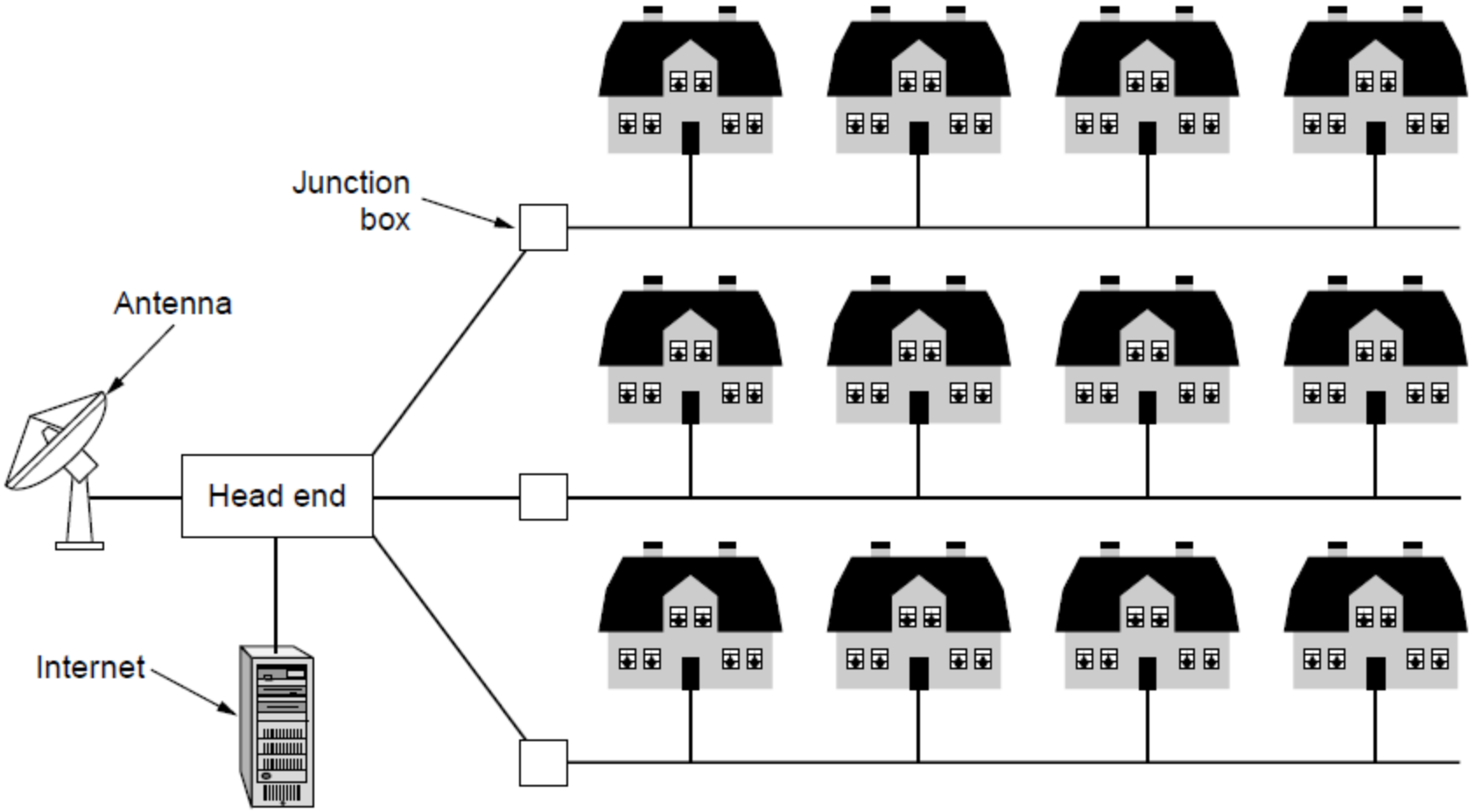
Old: BNC connector for coaxial cable

New: RJ45 for twisted pair cable

- Most of them use copper wires, but some use optical fiber.
- LANs run at speeds of 100 Mbps to 10 Gbps, have low delay
- The topology of many wired LANs is built from point-to-point links
- IEEE 802.3, popularly called **Ethernet**

MAN

- MAN (Metropolitan Area Network) covers a city
- The best-known examples of MANs are the cable television networks.
- The same system could be seen in cases where internet is distributed through cables.
- Signals are fed into centralized cable known as headend.


Junction box
Antenna
Head end
Internet

WAN

- A WAN spans a **large geographical area**, often a **country** or **continent**
- The rest of the network that connects hosts is then called the **communication subnet,** or just **subnet**
- **Transmission** lines move bits between machines. They can be made of **copper wire, optical fiber, or even radio links**
- **Switching elements** are specialized computers that connect two or more transmission lines
- Usually in a WAN, the hosts and subnet are owned and operated by ***different people***
-

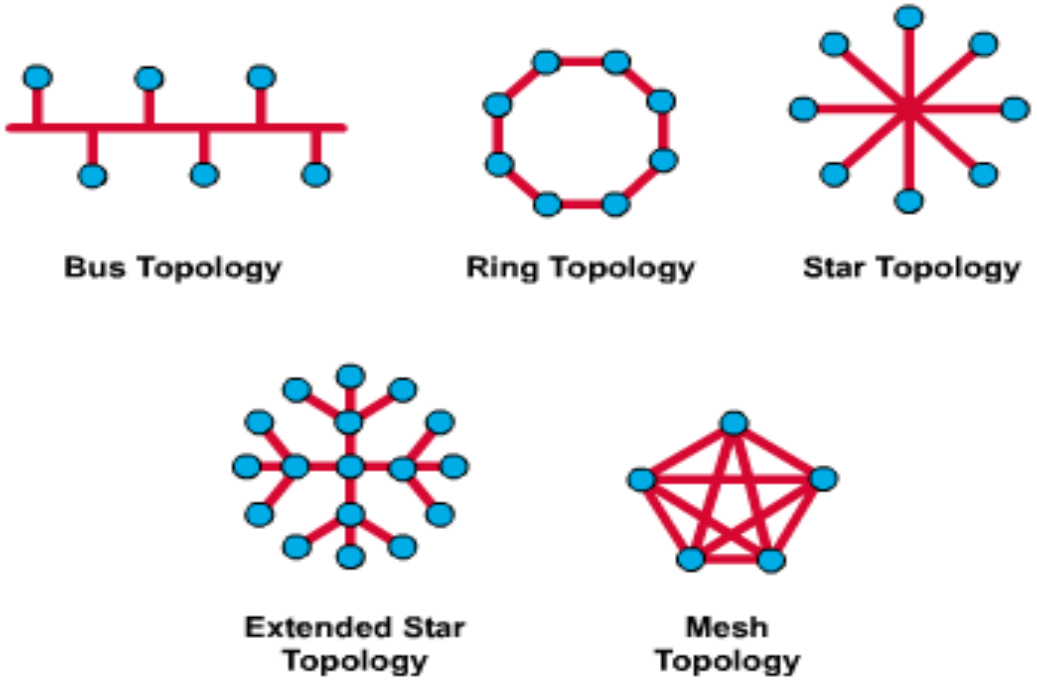
PAN

- Personal Area Network.
- The range is only a few meters.
- Bluetooth connections are an example.

Interprocessor distance	Processors located in same	Example
1 m	Square meter	Personal area network
10 m	Room	Local area network
100 m	Building	
1 km	Campus	
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1000 km	Continent	
10,000 km	Planet	The Internet

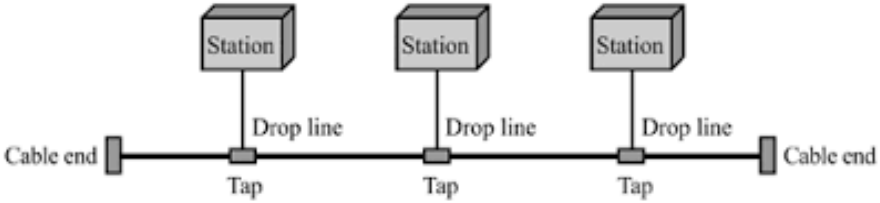
Network Topology

- **The network topology defines the way in which computers, printers, and other devices are connected. A network topology describes the layout of the wire and devices as well as the paths used by data transmissions.**



Bus topology

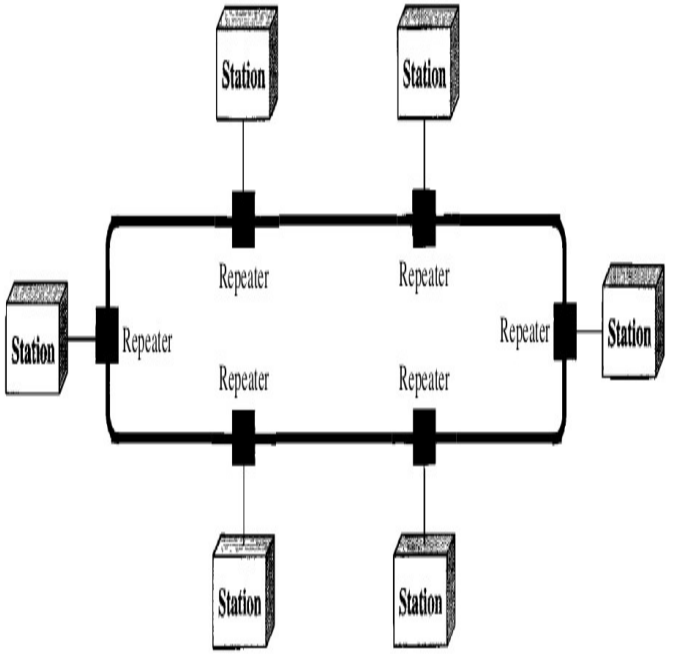
- Usually one long cable(medium) will serve as backbone.
- Signal travels using the cable.
- Nodes need tap points to connect to the medium.
- By adding taps and also as a result of propagation the strength will decrease.
- Require signal boosters.
- Any damage to the medium will impact systems on both sides of the medium.



Ref : Forouzan 4th edn..Page 9-12

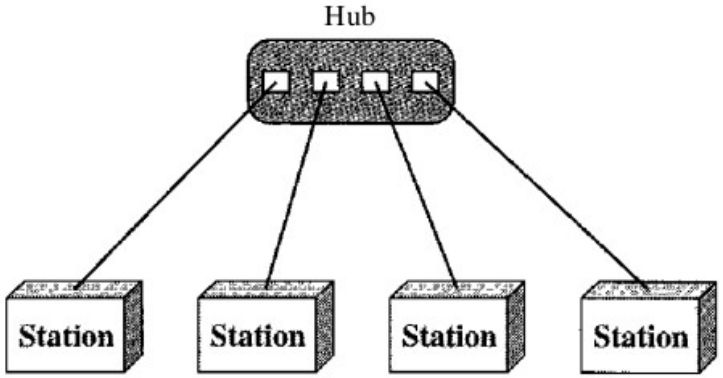
Ring topology

- One device typically linked to two neighbours.
- Normally the data passes in one direction from device to device before finally reaching the destination.
- A booster device is required to amplify the signal.
- Adding new nodes will be an issue.
- Can use bidirectional rings to acheive more efficient transmission



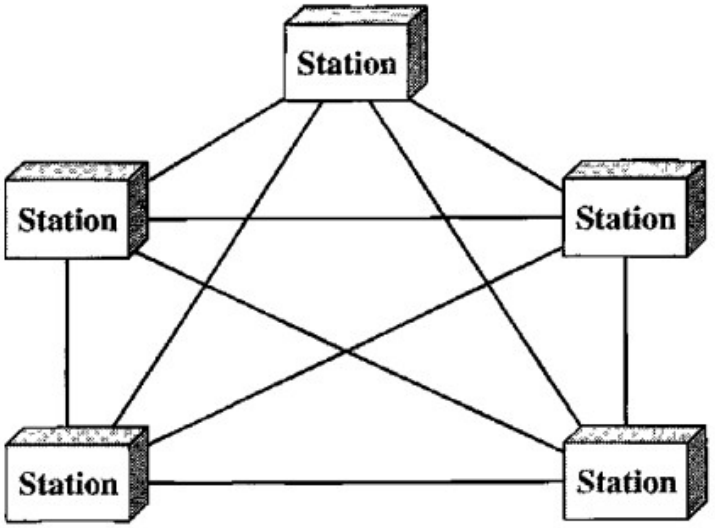
Star toplogy

- Nodes connected to a central node.
- The central node has the job to distribute the data among others.
- Usually the data is broadcasted and only the actual recipient will pick up the data.
- Adding new nodes are limited by the capacity of the central node.
- If central node fails,the network will collapse.



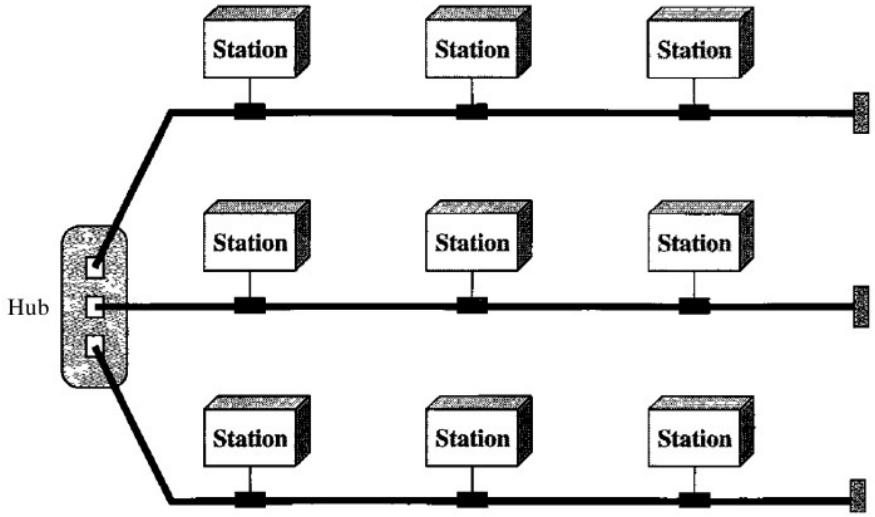
Mesh Topology

- In mesh topollogy all the nodes are connected to every other nodes.
- This will increase the cabling cost.
- Failure of medium will affect transmission only between the two end points of the medium.
- Fault identification is easy.



Hybrid topology

- Uses the best features of other topologies.
- Performed depending on specific requirements.
- Ex:- Star and Bus



Network hardware

- To connect multiple segments of networks into a larger one
- **Hub (Repeater)**
- A multi port repeater to enhance signal within the same LAN.

- **Switch**
- Like hub but with intelligent. Looks for sender and recipient address.
- Better performance.

- **Router**
- Forward data from one LAN to another

Internetwork

- Many networks exist in the world, often with **different hardware and software**
- A collection of interconnected networks is called an **internetwork** or **internet**.
- The **Internet** uses **ISP** networks to connect **enterprise**
- networks, **home** networks, and many other networks
- **Subnets, Networks, and Internetworks**
- Internet is formed when **distinct networks are interconnected**. (LAN, MAN, WAN)
- **Gateway**: provides the necessary translation

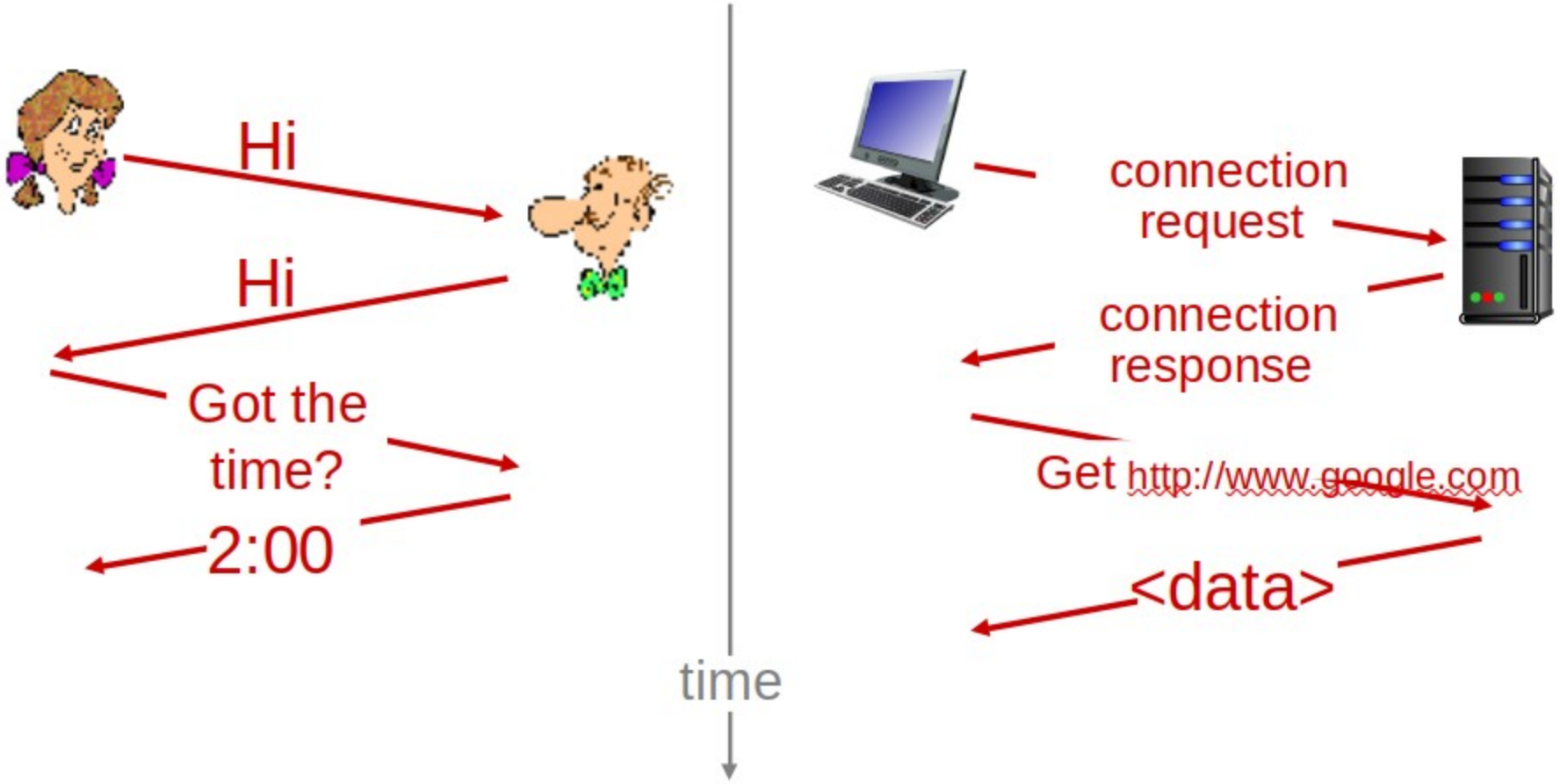
Things to think -1

- You are connected to a public wifi.
- There are other people who are using the same wifi.
- ***Q. How do you get the correct data destined to you ?***
- ***Q Is it possible to view information of others also ?***

Network Protocols

- A protocol refers to a set of rules which governs how an entire series of events should take place.
- In networking also a set of protocols define how data is transmitted and represented.
- Every device capable of networking should adhere to the protocol standards.
- Ex: HTTP [Hyper Text Transfer Protocol] defines how webpages are created and displayed by browsers.

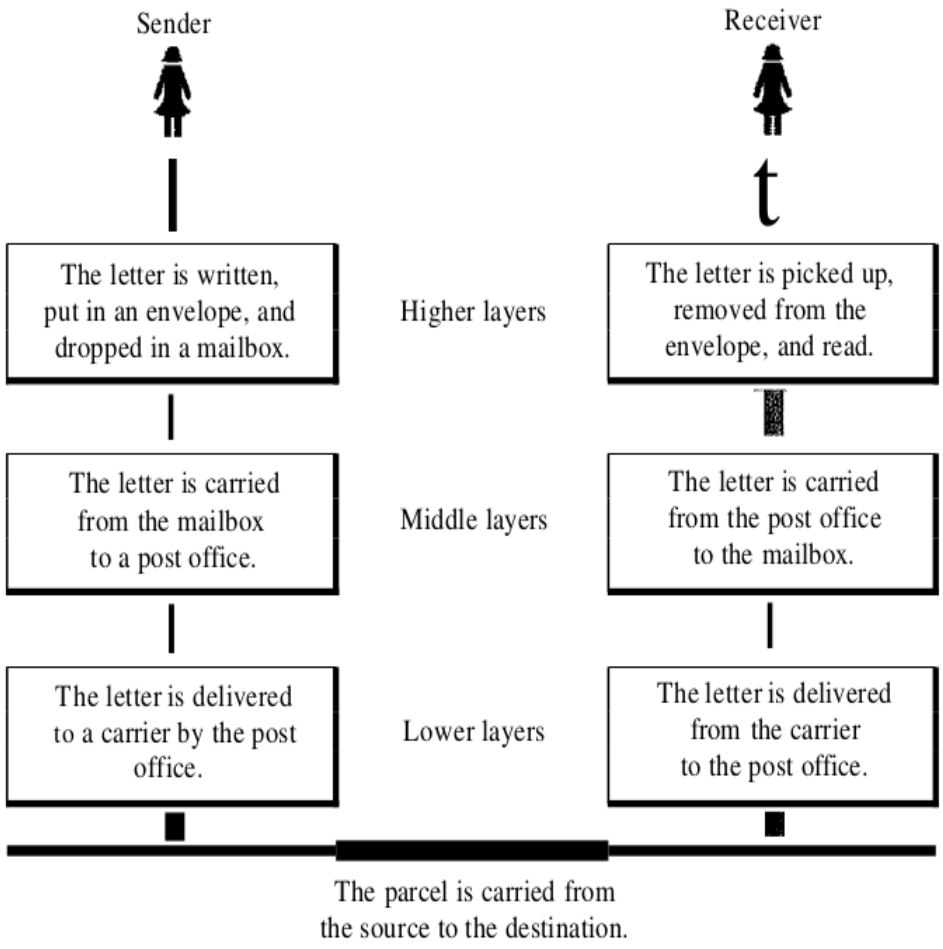
Human V/S Computer protocol



The concept of layering

- The process of sending and receiving data involves a lot of software and hardware components.
- The devices involved will be different in terms of software and hardware.
- Ex-Accessing saintgits.org from mobile phone.
- Each layer is designed to carry out specific task.
- Each layer has multiple protocols which ensure the working of different tasks.
- Changes /additions of functionalities will require change in one layer.

Real life example



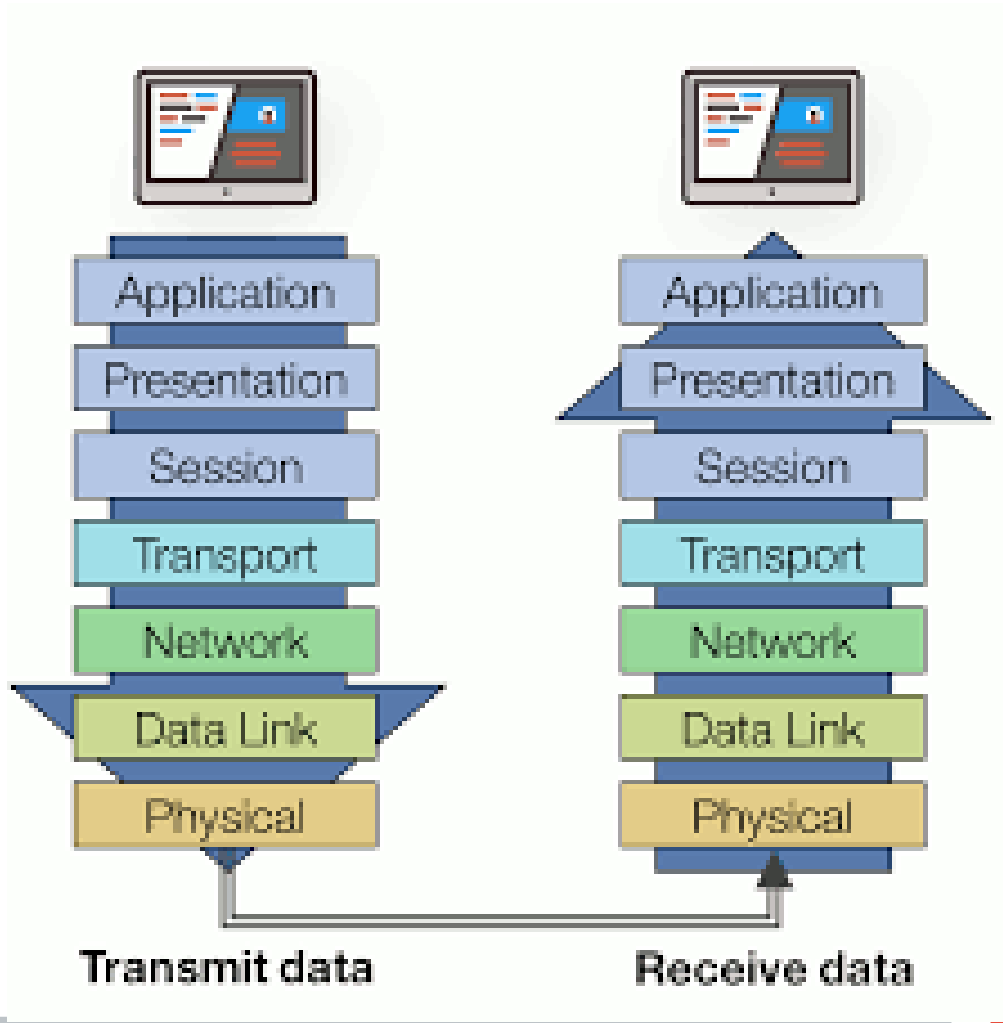
- Think of computers at both the ends !!

ISO-OSI Layering

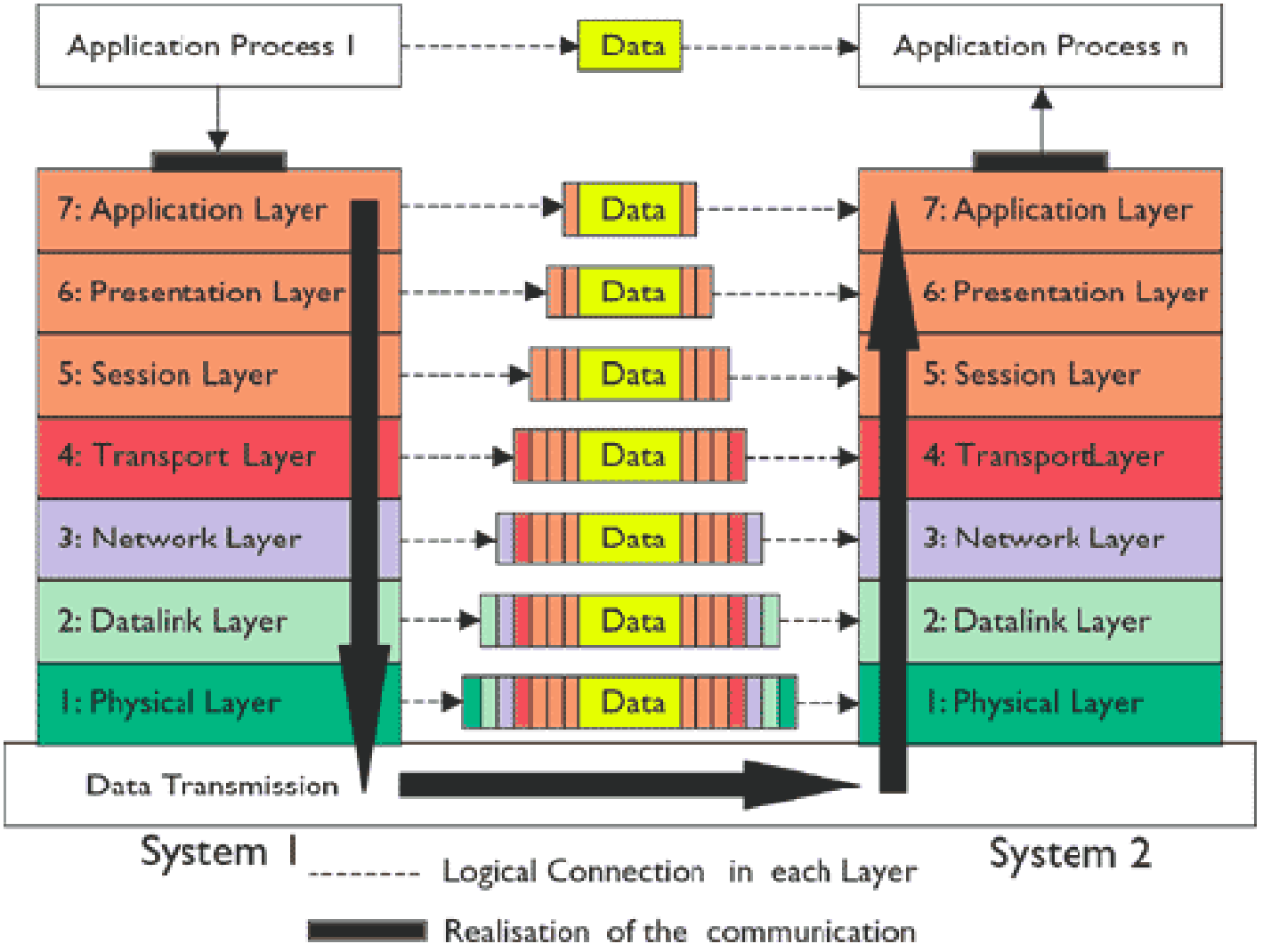
- One of the standard network layering standard.
- Established in late 1970 by **I**nternational **S**tandard **O**rganisation.
- **Open Systems Interconnection** (OSI) model was necessiated by the fact that the underlying hardware varied from organization to organization.
- The OSI model defined seven layers .
- Each layer defines its own protocols to aid in transferring data.

Ref : -Data Communication & Networking – Behrouz Forouzan

ISO-OSI Layers

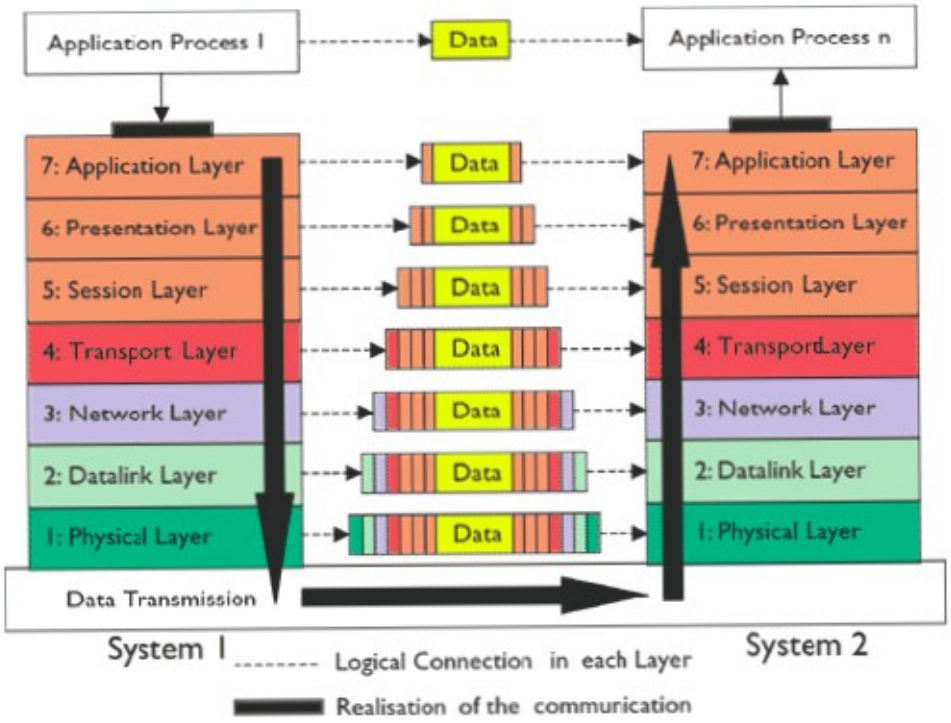


Contd..


Application Process I
Data
Application Process n
7: Application Layer
6: Presentation Layer
5: Session Layer
4: Transport Layer
3: Network Layer
2: Datalink Layer
1: Physical Layer
Data
Data
Data
Data
Data
Data
Data
7: Application Layer
6: Presentation Layer
5: Session Layer
4: TransportLayer
3: Network Layer
2: Datalink Layer
1: Physical Layer
Data Transmission
System I
System 2
Logical Connection in each Layer
Realisation of the communication

Data in each layer

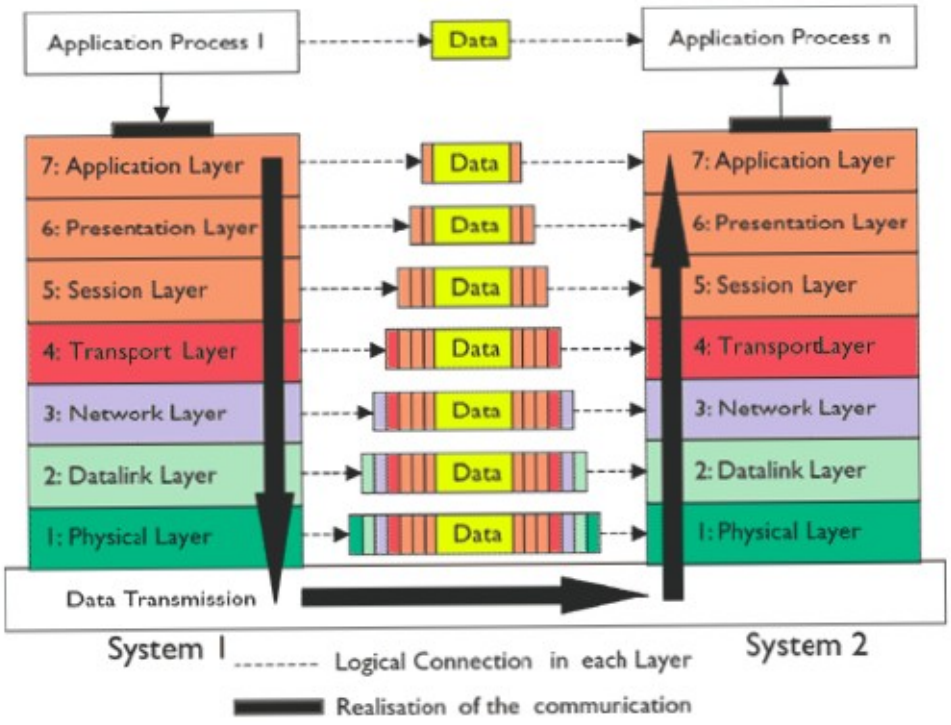
- Sender->data moves from application layer to physical layer.
- On the receiver it moves in the reverse direction.
- On moving down each layer adds extra information along with the data.
- Only physical layer has actual **physical** connection.



System 1-> Sender.
System 2-> Receiver.

Contd..

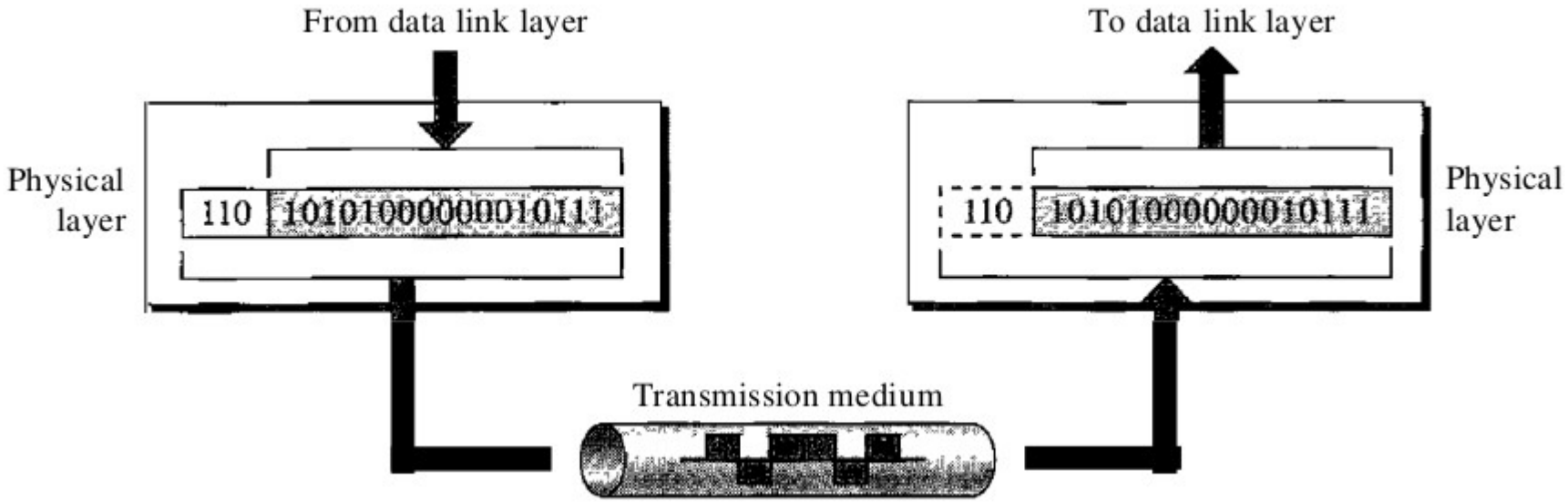
- The extra information added at the beginning is called Header.
- Those at the end are called trailer.
- Layer at any level treats data+extra information as its input data.
- The sender adds header/trailer.
- The receiver side reads the extra information and understands how to process the data.
- The receiver removes corresponding header/trailer before passing it to upper layers.



Some protocols will not add trailer

Physical layer

- Deals with transmitting data over a medium.
- Deals with the electrical and mechanical aspects of transmitting the bit stream.
- The data+header+trailer will be converted to 0’s and 1’s.
- A Zero means a signal low and One means a signal high.



Physical layer-Functions

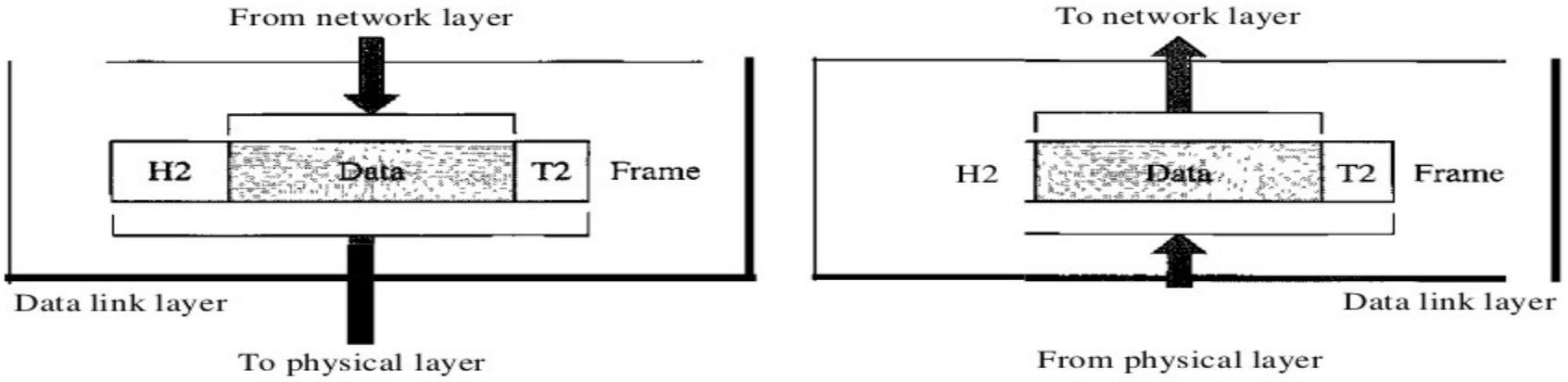
- Physical characteristics of interfaces and medium
  - Defines the type of medium and its specification.
- Encoding of bits.
  - Defines how 0 and 1 are changed to signal.
- Data rate
  - Number of bits send /received per second.
- Synchoronization of bits.
  - The sender and receiver should strike a synchronization so that the data is transmitted in correct order and rate.

Physical layer-Functions

- Line configuration
  - Concerned with connecting devices to medium.
- Physical topology
  - Concerns with topology specifc settings.
- Transmission mode.
  - Deals with the direction of transmission.
  - Simplex- One can send other can receive
  - Half duplex- Both can send and receive.But one at a time
  - Full duplex -Both can send and receive at the same time.

Data link layer

- This layer deals with creating a reliable physical link.
- The data+header+trailer in a data link layer is referred to as a **Frame.**
- Deals with delivering data to correct hardware interface



Data link layer - Functions

- Physical addressing.
  - Data link layer adds the physical addrerss of the devices. [Device interface]
  - This helps in delivering frames to the correct device interface.
- Flow control
  - The speed of the sender has to be regulated so as not to overwhelm the receiver.
- Error control
  - Incorporates techniques to find error in the bit stream and retransmit frames with errors.
- Access Control
  - When more than one device accesses the medium,datalink layer protocols determine who has access.

Network layer

- Network layer manages delivery of data across different networks.
- The data+header+trailer is reffered to as a **packet**.
- Network layer protocols contain the network address of the device (Ex: IP address).
-

Network layer- Functions

- Logical addressing.
  - Once the data passes one network,proper source and destination addressing needs to be done so as to ensure delivery of data.
- Routing
  - When independent networks are connected together,network routing protocols ensure that the best data reaches the destination through the best route.
-

Transport Layer

- Responsible for process to process delivery of data.
- Each process will be given a unique identifier .

Transport layer-Functions

- Service point addressing.
  - Service point refers to the application which is either a sender or a receiver.
- Segmentation and reassembly.
  - The data is broken into smaller units before sending and are reassembled.
- Connection control
  - Some transmission require the sender and receiver to agree upon certain parameters before actual data transmission.

Transport Layer-Functions

- Flow control
  - The speed of the sender will be maintained so as to make sure that the receiver is not overwhelmed by the data.
- Error Control
  - When there is an error ,transport layer protocols ensure retransmission of those segments which has errors.

Session Layer

- Session layer establishes the necessary synchronization between the sender and the recepient.
- The protocols ensure that the proper parameters are established through dialog control.
- Ex:- Security key for applications.

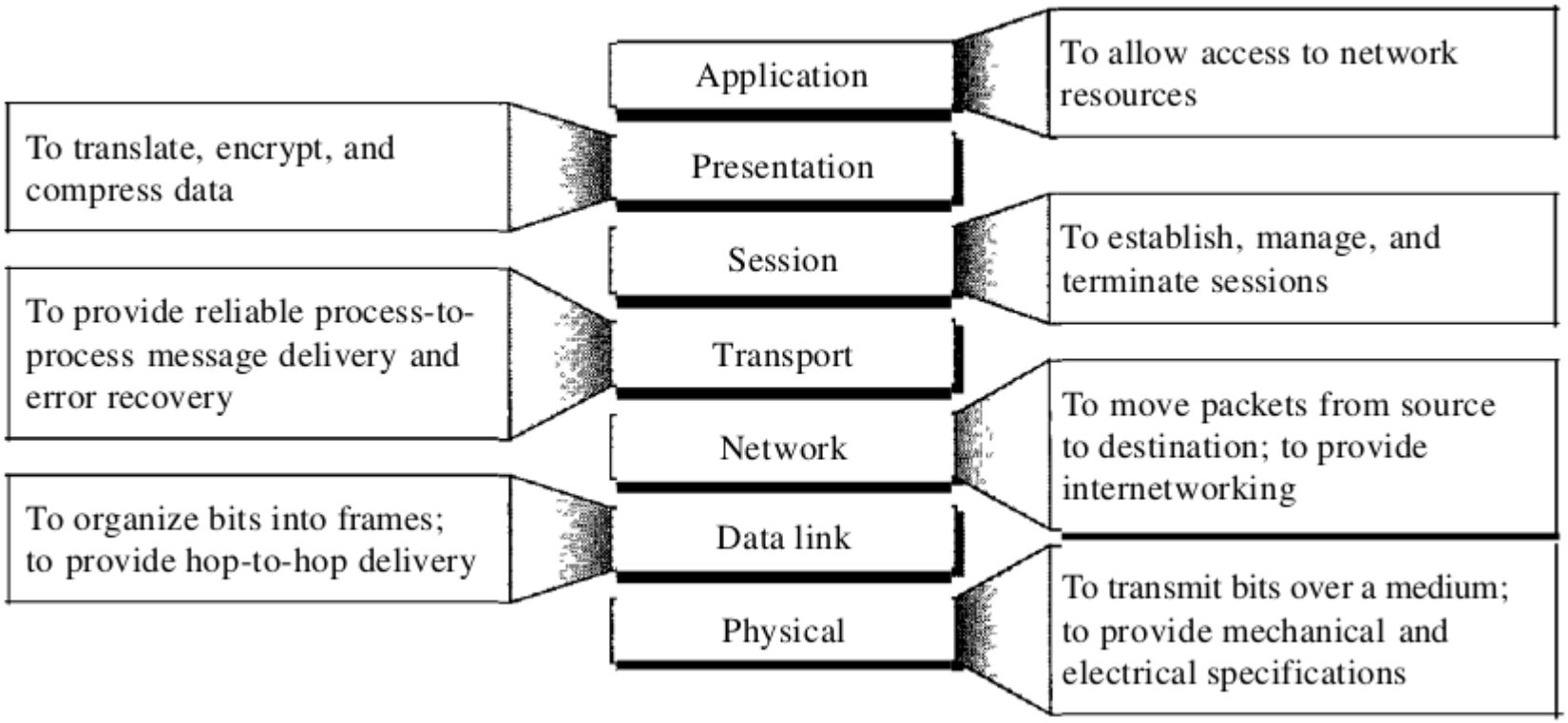
Presentation layer

- The layer is concerned with the syntax and semantics of the information exchanged.
- Translation
  - The applications might require some of the data to be properly translated.Translation can include simple conversion of numeric types also.
- Encryption
  - Deals with encrypting and decrypting the data.
- Compression
  - In order to reduce the number of bits transmitted compression techniques are employed at the sender.The same are decompressed at the other end.

Application Layer

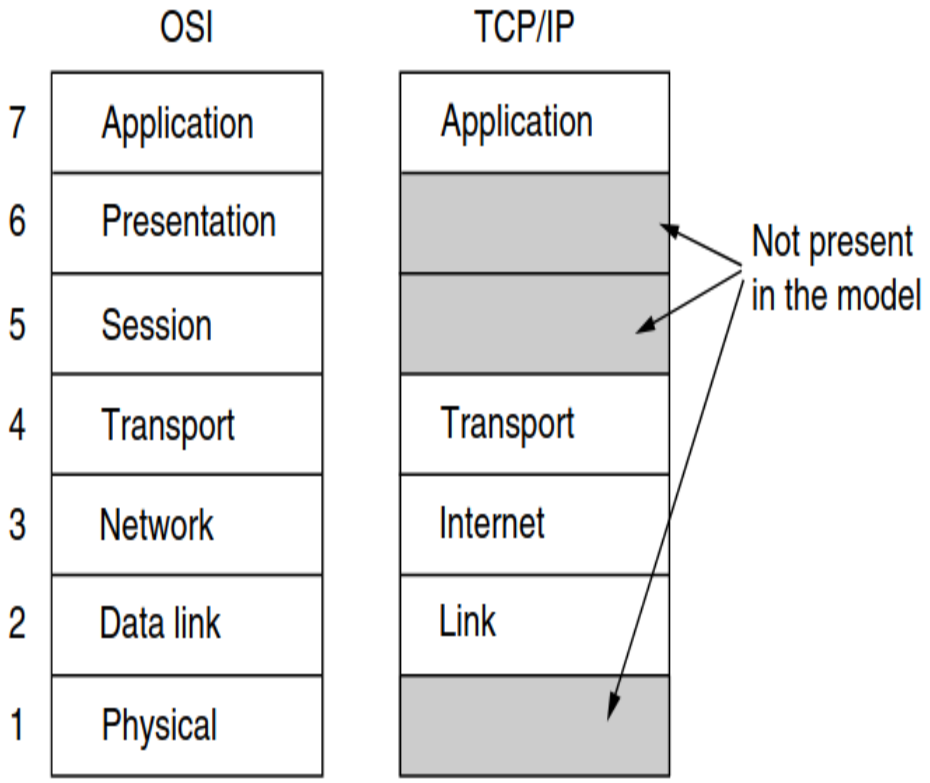
- Application layer protocols lets the user or the applications use the network.
- Some protocols provide a terminal [GUI/ Non GUI] to access the resources.
- Common services include mail services,directory services,file manipulation services.

ISO -OSI


Application
To allow access to network resources
To translate, encrypt, and compress data
Presentation
Session
To establish, manage, and terminate sessions
To provide reliable process-to-process message delivery and error recovery
Transport
Network
To move packets from source to destination; to provide internetworking
To organize bits into frames; to provide hop-to-hop delivery
Data link
Physical
To transmit bits over a medium; to provide mechanical and electrical specifications

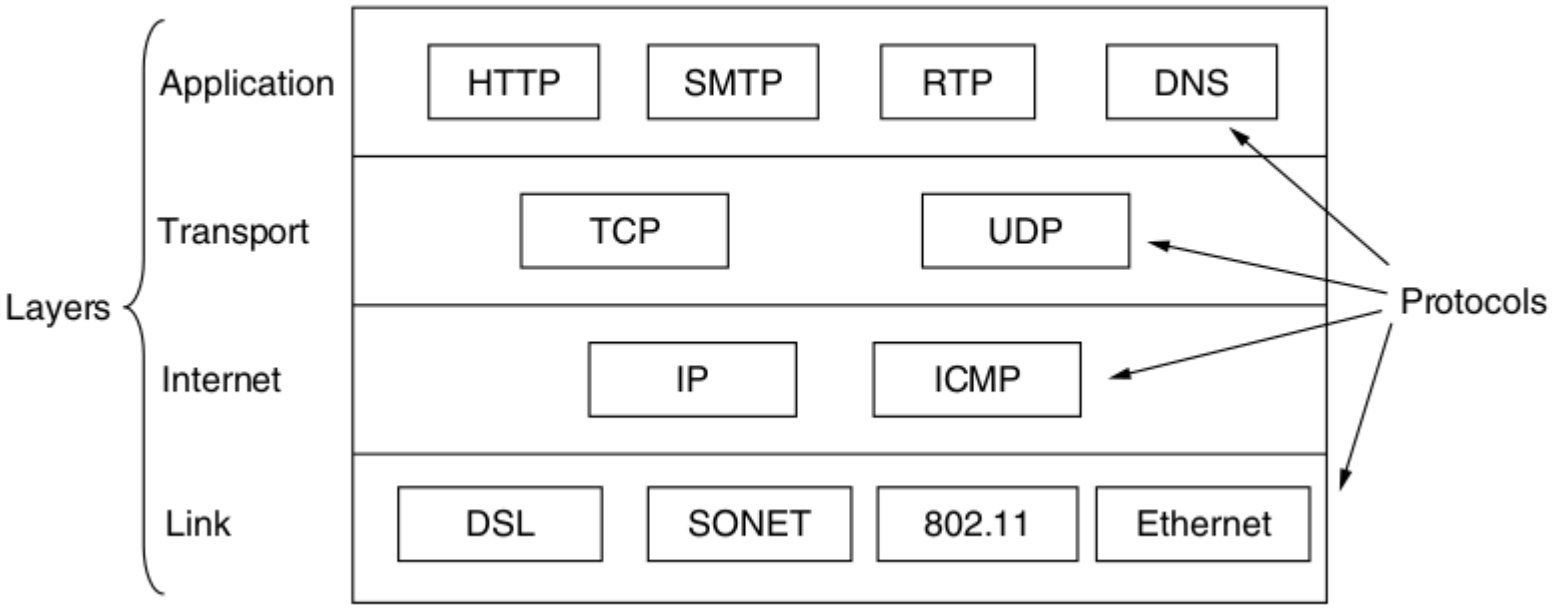
TCP/IP Layering

- Transmission Control Protocol/ Internet Protocol
- The functions performed by Application,Presentation and session layer in OSI layering model is performed by Application Layer.
- The functions of physical and datalink layer also are combined.
- So Contains only 4 layers.



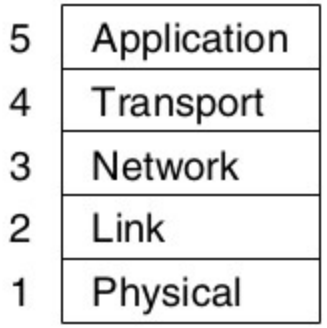
TCP/IP Layering

- The strength of TCP/IP layering is the protocols specified in each layer.
-



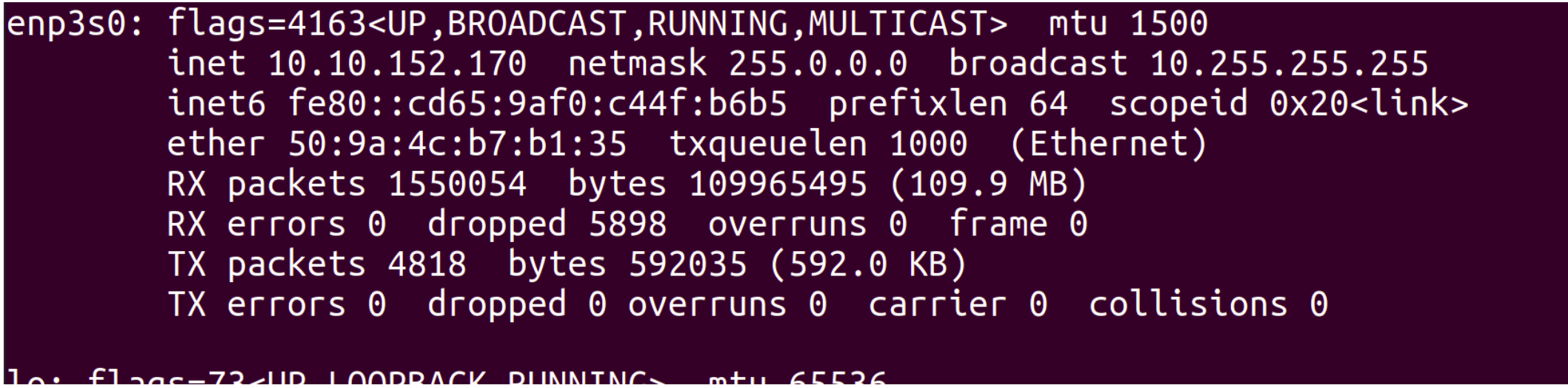
A hybrid layered model

- A hybrid model comprising of 5 layers is generally used in Internet.
- Some textbooks also use the same reference.



Type of addresses

- In modern networks any transmission involves the usage of 3 major addresses.
- **1. Device addresses**
- Every node that access the network has a specific hardware part that can deal with the transmission.
- This hardware device has an address which is assigned during manufacturing.
- This address is permanent.
- Ex:- MAC Address



- The *ether* part gives the mac address on a laptop using ethernet/LAN.

2.IP address

```
enp3s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.152.170  netmask 255.0.0.0  broadcast 10.255.255.255
        inet6 fe80::cd65:9af0:c44f:b6b5  prefixlen 64  scopeid 0x20<link>
        ether 50:9a:4c:b7:b1:35  txqueuelen 1000  (Ethernet)
        RX packets 1550054  bytes 109965495 (109.9 MB)
        RX errors 0  dropped 5898  overruns 0  frame 0
        TX packets 4818  bytes 592035 (592.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
```

- The inet part gives the IP address in our network.
- The inet6 gives the Ipv6 address.
- The IP address will change based on the network.

3.The port number

```
TCP 10.10.152.170:56556->142.250.196.68:443 (ESTABLISHED)
TCP 10.10.152.170:50656->104.21.7.83:443 (ESTABLISHED)
TCP 10.10.152.170:48410->35.244.247.133:443 (ESTABLISHED)
TCP 10.10.152.170:50488->142.251.12.155:443 (ESTABLISHED)
TCP 10.10.152.170:49180->34.120.115.102:443 (ESTABLISHED)
TCP 10.10.152.170:59632->142.250.193.110:443 (ESTABLISHED)
TCP 10.10.152.170:45732->44.239.205.250:443 (ESTABLISHED)
TCP 10.10.152.170:35056->142.250.196.67:443 (ESTABLISHED)
```

- The number after **:** is the port number.
- The application will be using this number to send/receive the data.

Common port numbers

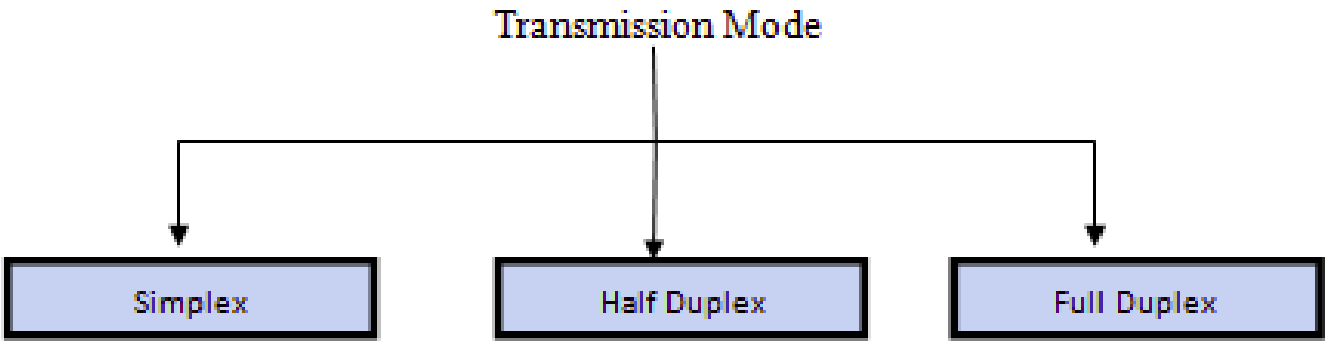
Port Number	Protocol
20, 21	File Transfer Protocol (FTP)
22	Secure Shell (SSH)
23	Telnet Protocol
25	Simple Mail Transfer Protocol (SMTP)
53	Domain Name System (DNS)
67, 68	Dynamic Host Configuration Protocol (DHCP)
80	HyperText Transfer Protocol (HTTP)
110	Post Office Protocol (POP3)
137	NetBIOS Name Service
143	Internet Message Access Protocol (IMAP4)
443	Secure HTTP (HTTPS)
445	Microsoft-DS (Active Directory)

Connection Oriented Transfer

- The sender and the receiver agree upon certain parameters before transmission.
- If the receiver finds an error the sender has to resend the data.
- On receiving any data,the receiver has to send an acknowledgment.
- These steps ensure reliability but adds delay.
- When the application cannot tolerate delay use connectionless transmission.
- Done in transport layer and is independent of the medium.

Modes of Communication

- Defines how data is transfered.



Simplex Transmission

- Communication between sender and receiver happens only in one direction.
- There is no mechansim to transmit data in the other direction.
- Can utilize the full capacity of the channel.
- Ex: - Keyboard to CPU transfer

Half duplex

- The communication between sender and receiver can happen in both directions.
- **But only one can transmit at a time.**
- Ex :- Walkie Talkie transmission

Full duplex transmission

- In full duplex transmission both the parties can transmit at the same time.
- Ex:- Normal Telephone conversation.

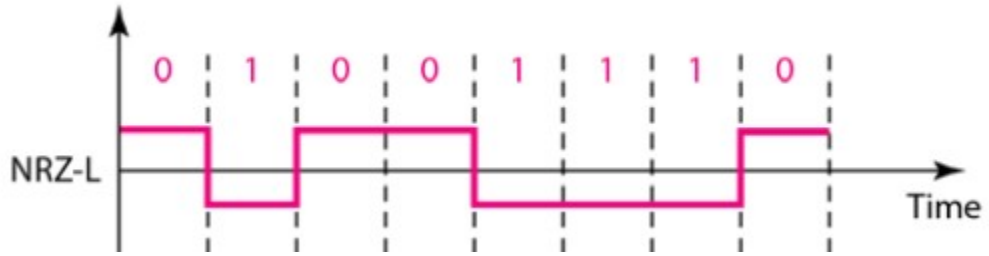
Basis for Comparison	Simplex	Half Duplex	Full Duplex
Direction of Communication	Unidirectional	Two-directional, one at a time	Two-directional, simultaneously
Send / Receive	Sender can only send data	Sender can send and receive data, but one a time	Sender can send and receive data simultaneously
Performance	Worst performing mode of transmission	Better than Simplex	Best performing mode of transmission
Example	Keyboard and monitor	Walkie-talkie	Telephone

Encoding schemes

- Encoding converts data in one form to the other.
- In physical layer digital data is transformed so as to convert to digital signals.
- The schemes define how a signal low or high can be interpreted as a bit.
- The sender and receiver has to synchronise their signal clock prior to transmission.
- This helps to define bit boundaries during transmission.

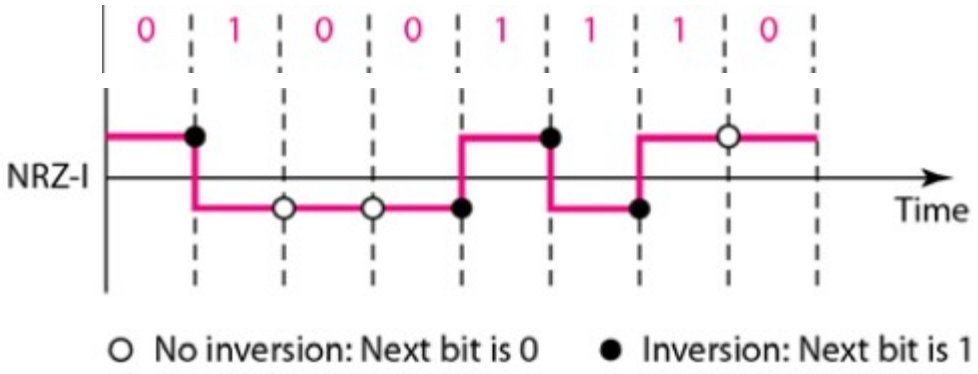
Non Return to Zero(NRZ) - Encoding

- Positive volt encodes a Zero.
- Negative volt encodes a One.
- This scheme is also refered to as NRZ-L (L-->Level)
-



NRZ-I

- At the bit start , a transition is encoded as a One.
- If there are no transitions ,then a Zero.

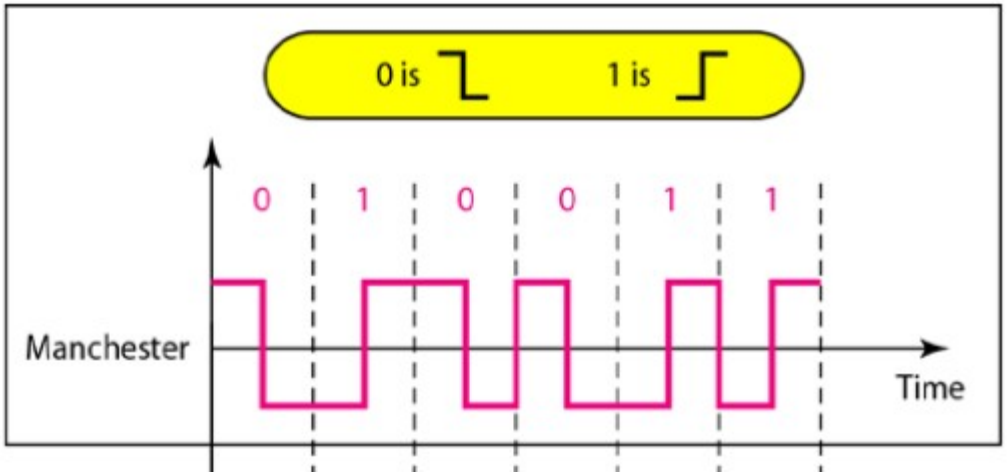


Issue of base line wandering

- The received power is calculated based on the average of the power received in comparision to the ground.
- If a large string of Zero or One is encoded using NRZ - I, the signal power will not change.
- This causes a change in average power at the receiver.
- This might cause the receiver to decode wrong values.

Manchester Encoding

- A logic one is represented by a low to high transistion.
- A logic zero is represented by high to low transition.
- The transitions happen in the middle of the bit boundary.
- Used in ethernet / twisted pair.

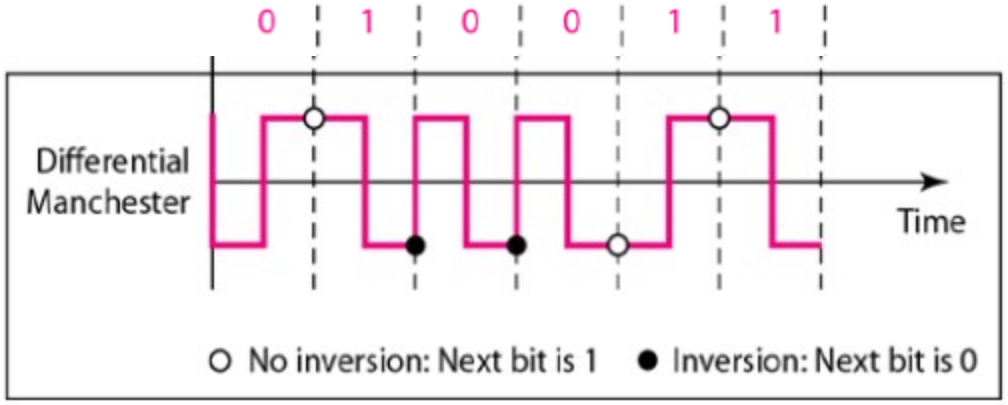


One word of caution !!

- There are two versions of Manchester encoding that is referred in text books.
- The other version considers high to low as 1 and vice versa.
- You may write your assumptions before attempting the encoding.

Differential manchester encoding

- Transitions will happen in between the bit boundary.[No matter the bit]
- Bit values determined at the **beginning** of the boundary.
- A transtion encodes a Zero.
- No transition encodes a One.



4B / 5B Coding

- Considers a 4 bit block of input bits.
- The 4 bits are mapped to a 5 bit sequence.
- Mainly used along with other encoding schemes.
- The sequence is created so as to avoid continous Zero/One.

Data Sequence	Encoded Sequence	Data Sequence	Encoded Sequence
0000	11110	1000	10010
0001	01001	1001	10011
0010	10100	1010	10110
0011	10101	1011	10111
0100	01010	1100	11010
0101	01011	1101	11011
0110	01110	1110	11100
0111	01111	1111	11101

Network performance measures

- Network performance indicates the capability of a network in transmitting the data.
- Various factors affect the performance.
- There are defined metrics by which the performance is measured.
-

1.Bandwidth

- Bandwidth refers to the number of bits per second that a channel /network / medium can transmit.
- This represents the capacity of the channel.
- The value also gives an idea of the upper limit.
- Represented as *bps -->bits per second* and its higher order.

2.Throughput

- The value represents how fast the data can **actually** travel.
- Basic unit is *bps.*
- If the bandwidth is **B *bps*** ,throughput **T** will be less than **B.**
-

3.1 Propagation time

- The time taken by a bit to travel from source to destination.
- Propagation time= Distance / Propagation speed.

3.2 Transmission Time

- The time taken for one unit of message to reach destination. [Several bits]
- One message will conatin several bits

3.3 Queing Time

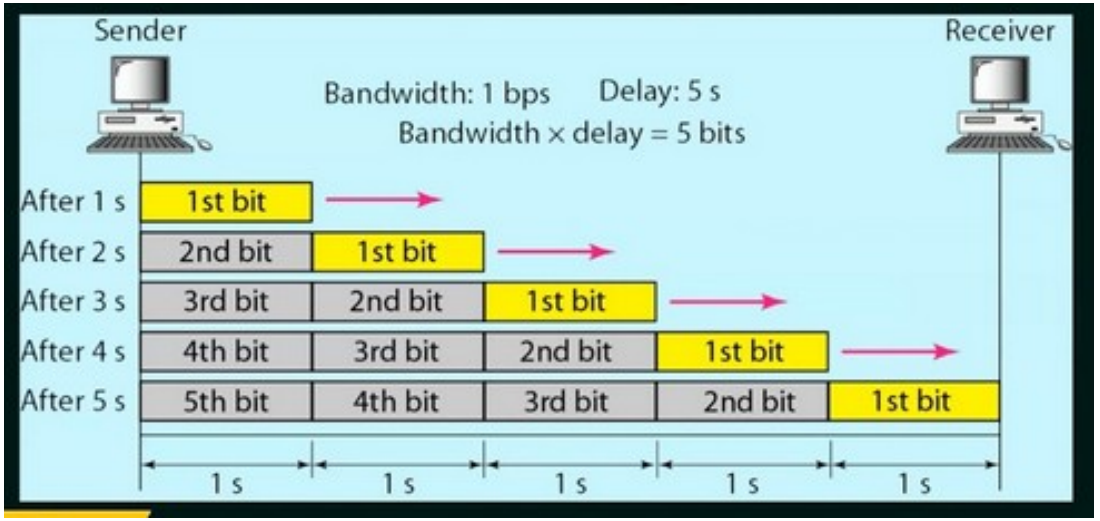
- The devices cannot match the speed of transmission in most cases.
- So they employ a queue to store the data before consuming it.
- Queuing will be required because of load on the network also.
-

Latency /Delay

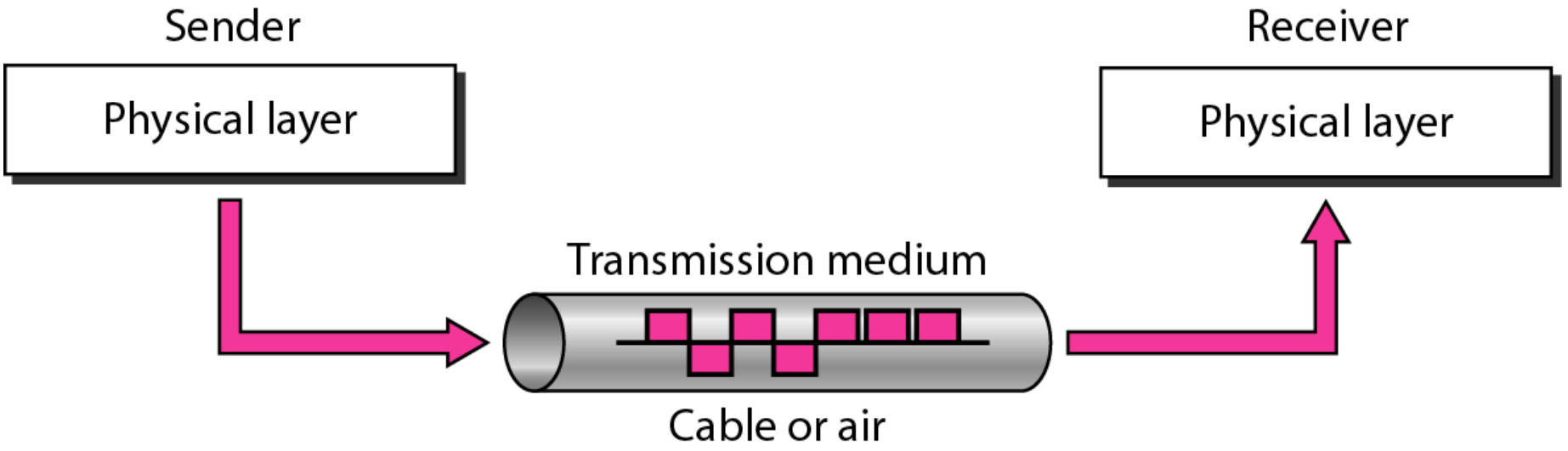
- The entire time taken for an entire message to start from sender and reach the destination.
- Latency=Propagation Time+Transmission time+queing time+processing delay.
- Processing delay is the time taken to process the data.

Bandwidth Delay Product

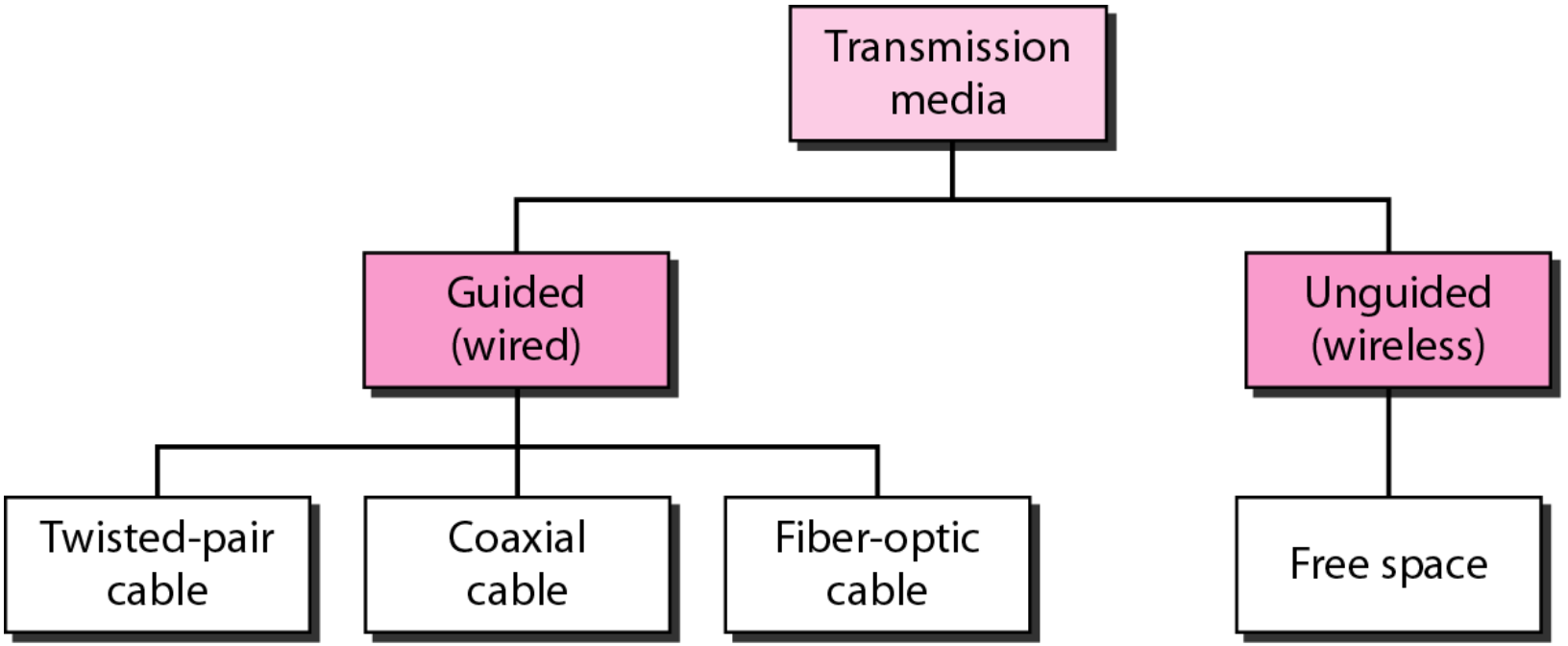
- The product of bandwidth and delay determines the number of bits that can fill the link.



Transmission Media

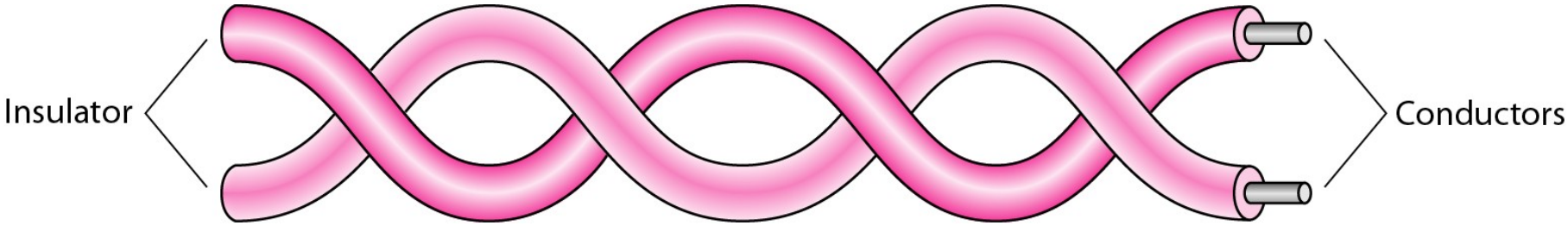


Classification



Guided Media

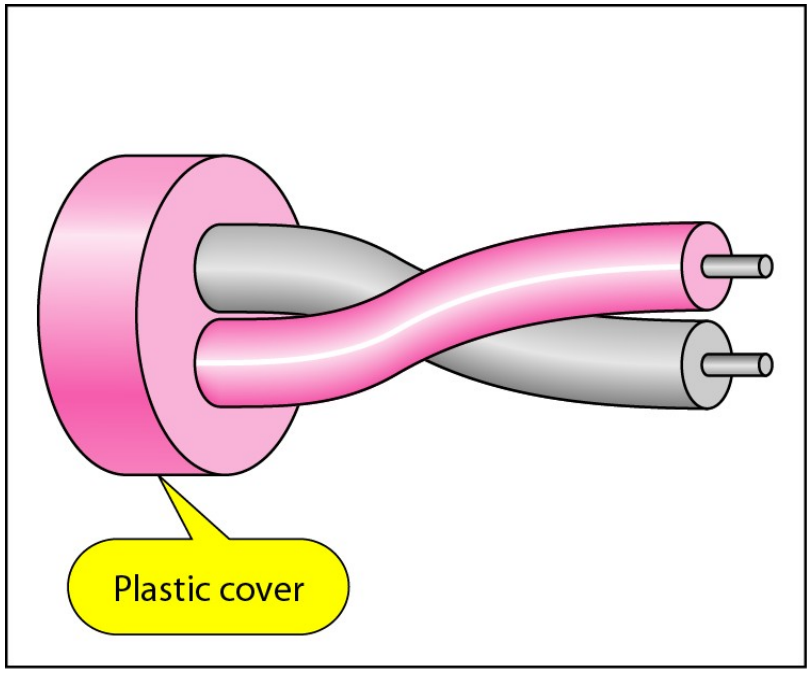
- ***Guided media, which are those that provide a conduit from one device to another, include twisted-pair cable, coaxial cable, and fiber-optic cable.***



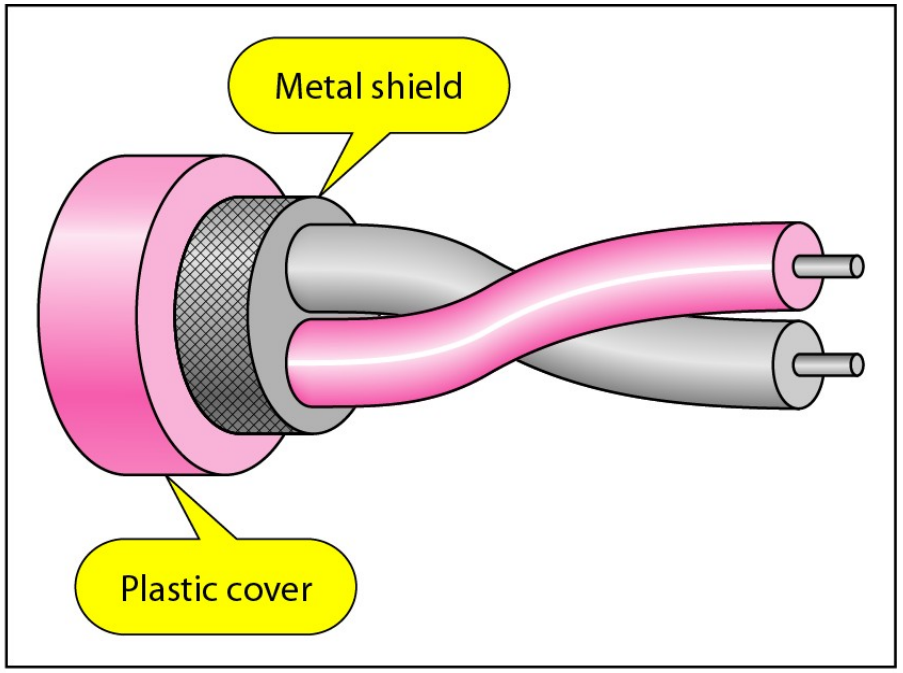
- The above is a Twisted Pair cable**.**
- The twisting is done to cancel out any interference.

Sheilded and Unsheilded Twisted Pair

UTP	STP
UTP stands for Unshielded twisted pair.	STP stands for Shielded twisted pair.
In UTP grounding cable is not necessary.	While in STP grounding cable is required.
Data rate in UTP is slow compared to STP.	Data rate in STP is high.
The cost of UTP is less.	While STP is costlier than UTP.
In UTP much more maintenance are not needed.	While in STP much more maintenance are needed.
In UTP noise is high compared to STP.	While in STP noise is less.
In UTP the generation of crosstalk is also high compared to STP.	While in STP generation of crosstalk is also less.
In UTP, attenuation is high in comparison to STP.	While in STP attenuation is low.
In UTP, speed offered is about 10 to up to 1000 Mbps.	While in STP speed offered is about 10 to up to 100 Mbps.
It is used for data transmission within short distance such as for home and	Generally used for connecting organizations over a long distance.

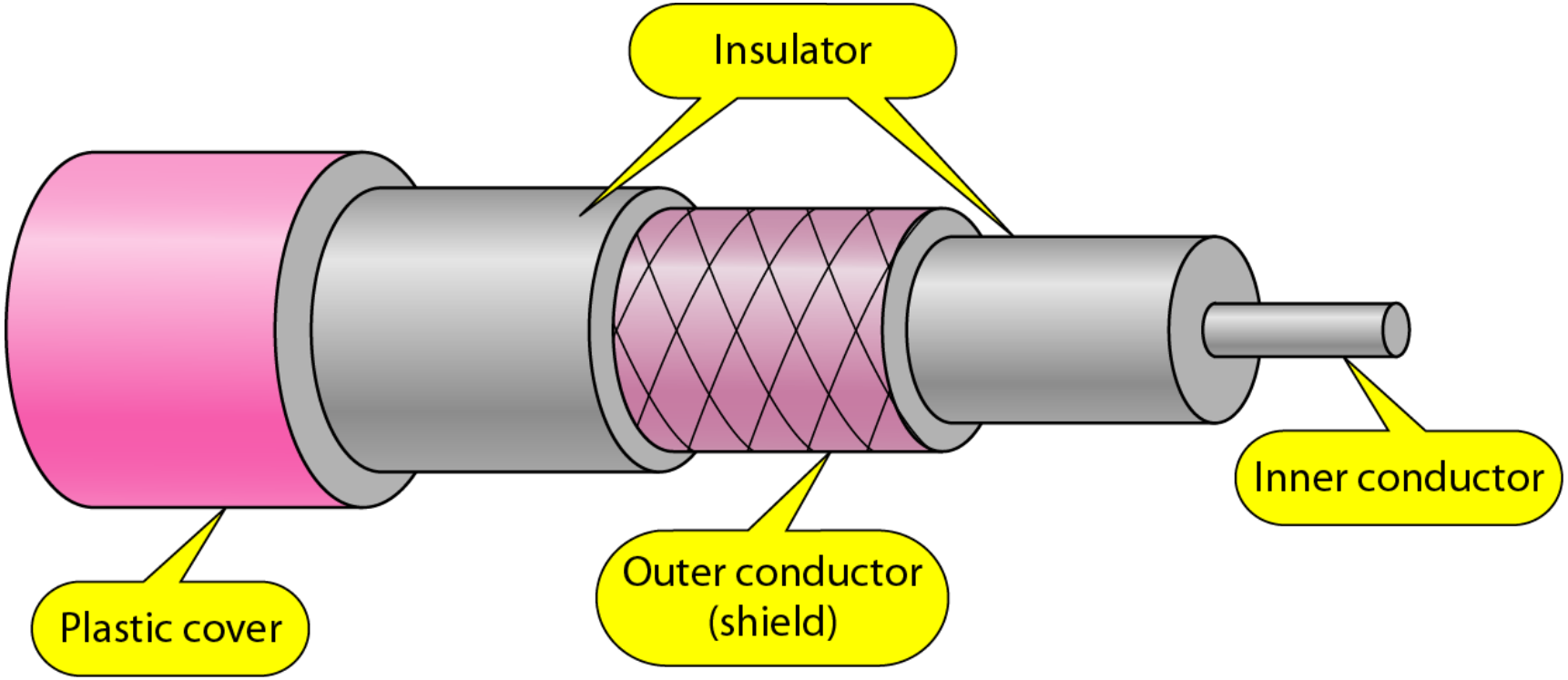


a. UTP



b. STP

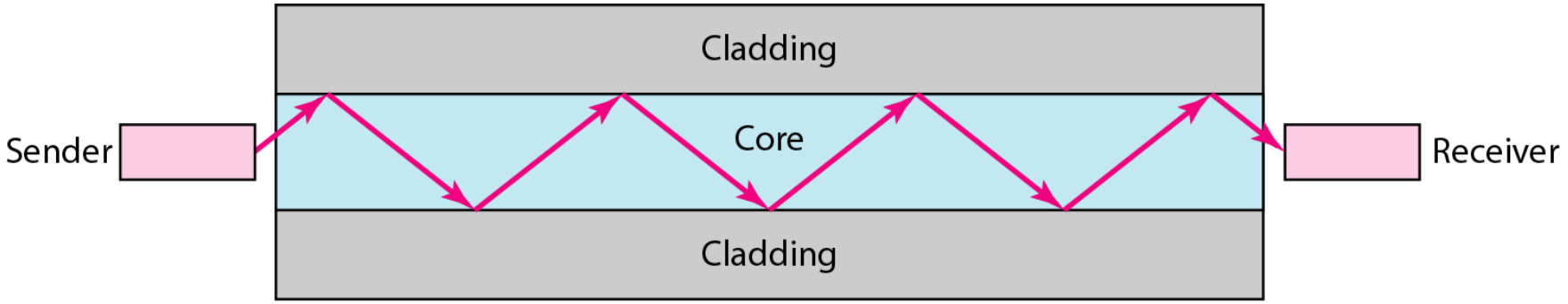
Co-Axial Cable



- Coaxial cable is used for both analog and digital data transmission.
- It has higher bandwidth, hence it can support mixed range of services.
- Because of its insulation, coaxial cable has lower error rates.
- Greater spacing between amplifier is possible.
- It uses for longer distances at higher data rates.
- Easy to handle.
- Relatively inexpensive as compared to optic fibre cables.

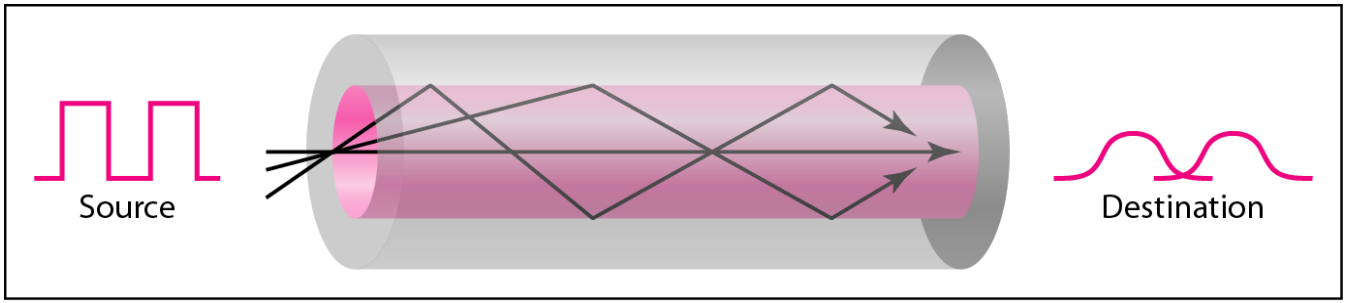
Optical Fiber

- Converts data to light and uses principles of reflection to transmit the data.

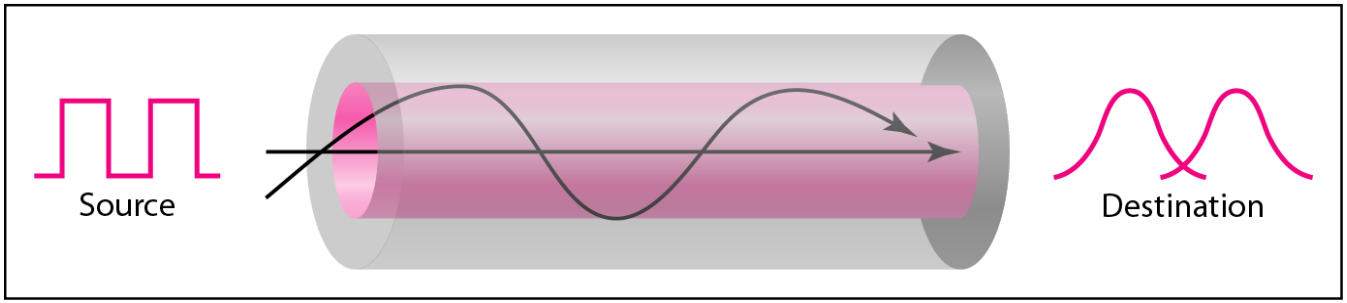


- Bandwidth is above copper cables
- Less power loss and allows data transmission for extended distances
- Optical cable is resistance for electromagnetic interference
- Fiber cable is sized as 4.5 times which is best than copper wires
- As cable are lighter, thinner, in order that they use less area as compared to copper wires
- Optical fiber cable is extremely hard to tap because they don’t produce electromagnetic energy. These optical fiber cables are very secure for transmitting data.
- This cable opposes most acidic elements that hit copper wired also are flexible in nature.
- Light has fastest speed within universe, such a lot faster signals
- Fiber optic cables allow much more cable than copper twisted pair cables.
- Fiber optic cables have how more bandwidth than copper twisted pair cables.
- Fault detection can be difficult.

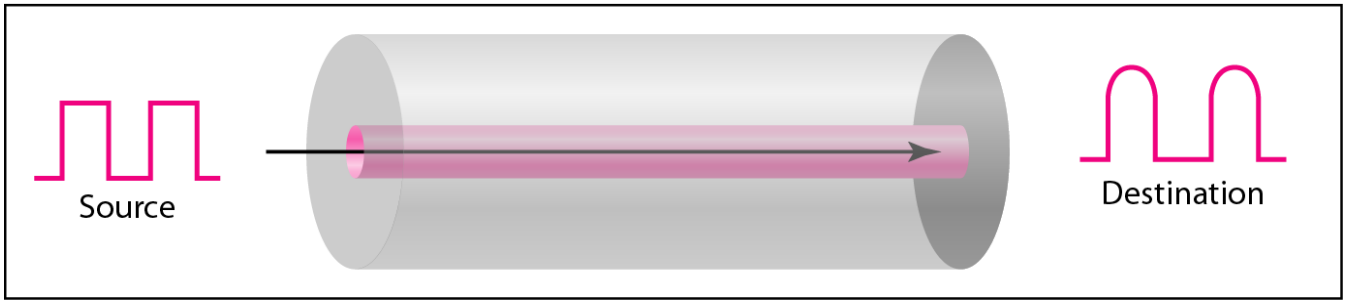
Modes



a. Multimode, step index



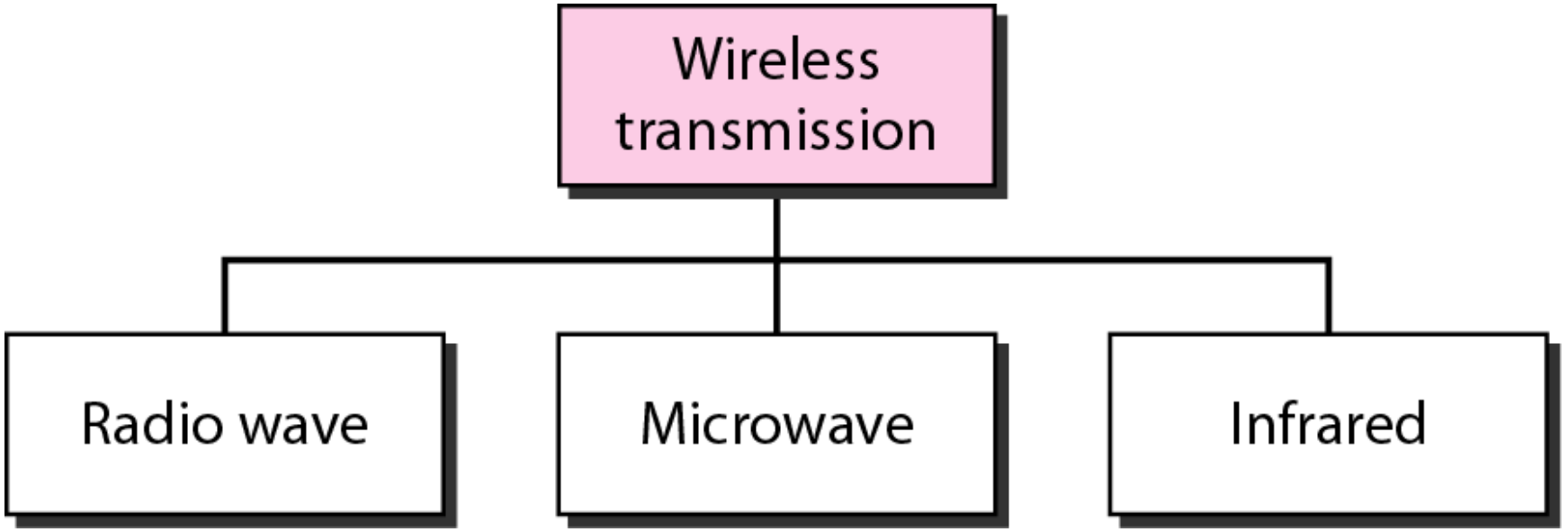
b. Multimode, graded index



c. Single mode

Unguided Media

- ***Unguided media transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication.***



Radio Waves

Radio waves are used for multicast communications, such as radio and television, and paging systems. They can penetrate through walls. Highly regulated. Use omni directional antennas

- The position of he receiver antenna is critical in good reception.

Microwaves

- Microwaves are used for unicast communication such as cellular telephones, satellite networks,and wireless LANs.
- Higher frequency ranges.Limited ability to penetrate walls.
- Use directional antennas - point to point line of sight communications.

Infrared Signals

- Infrared signals can be used for short-range communication in a closed area using line-of-sight propagation.

Properties of Wireless Channels

- Are subject to a lot more errors than guided media channels.
- Interference is one cause for errors, can be circumvented with high SNR.
- The higher the SNR the less capacity is available for transmission due to the broadcast nature of the channel.
- Channel also subject to fading and no coverage holes.