

CS3102 - Computer Networks

Mallikarjuna Nandi
Assistant Professor
Computer Science & Engineering
RGUKT- Ongole-AP

Unit 1- Syllabus

Unit - I

(7Contact hours)

Introduction: Network Hardware, Network Software, References Models. Physical Layer-Guided medium and unguided medium, topologies.

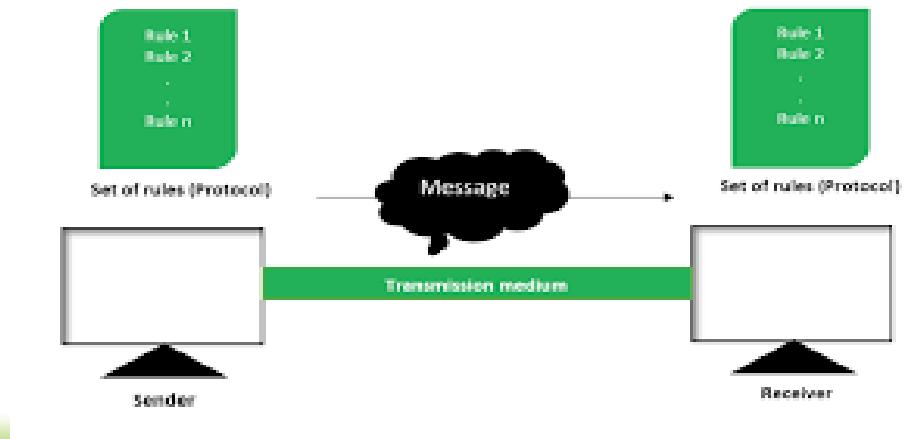
Course Learning Objectives:

- ❖ Build an understanding of the fundamental concept of computer networking.
- ❖ Formalize the student with the basic terminology of the computer networking.
- ❖ Introduce the advanced networking concepts.

Introduction

Computer Networks :

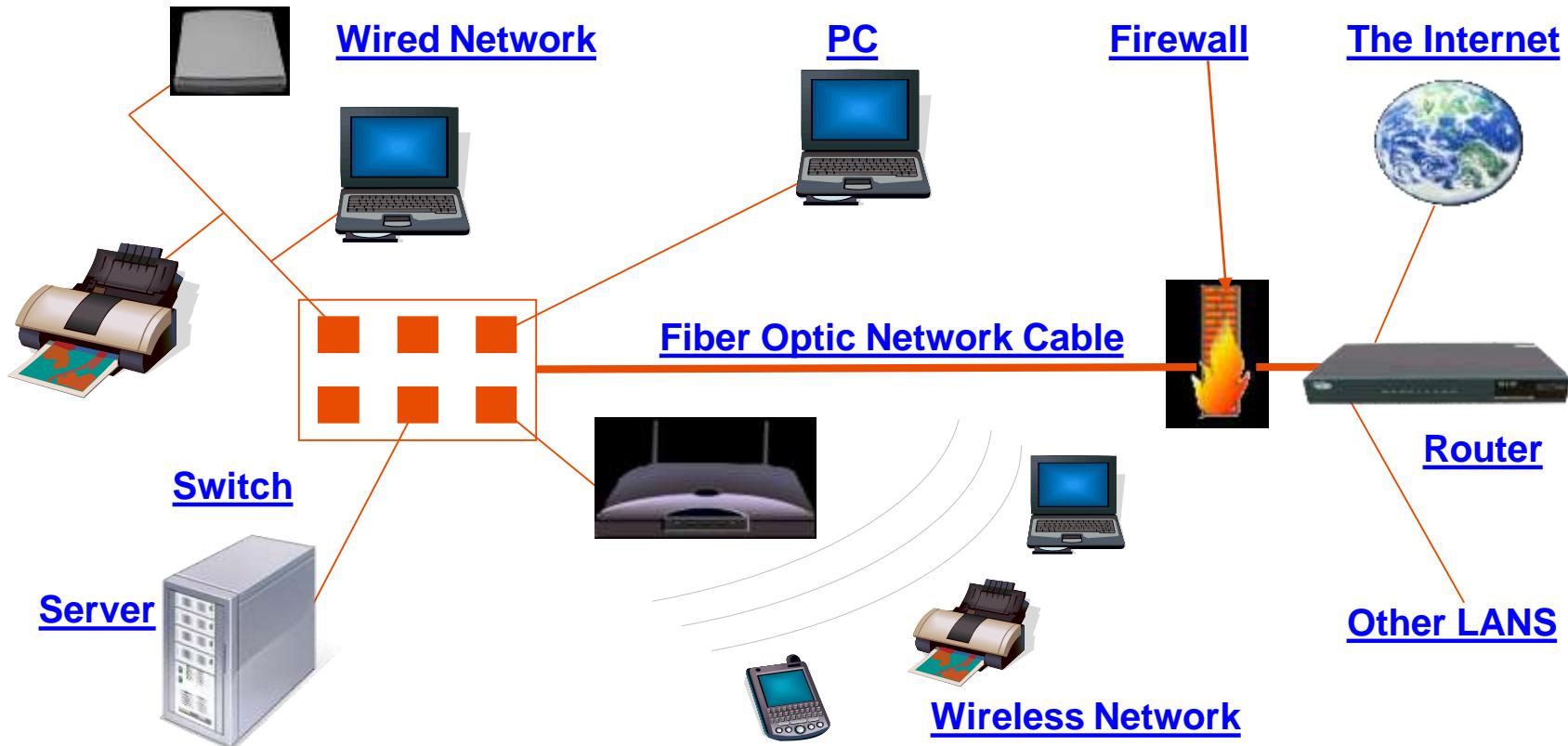
- A **computer network** is a group of computers/devices (**Nodes**) that use a set of common communication **protocols** for digital **interconnections** for the purpose of sharing resources located at different network nodes.



Introduction

- The **nodes** of a computer network may include personal computers, servers, networking hardware, or other specialised or general-purpose hosts.
- The **interconnections** between nodes are formed from a broad spectrum of telecommunication network technologies, based on physically wired, optical, and wireless technologies.
- A **communication protocol** is a set of rules for exchanging information over a network.

Computer Networks Block Diagram



Introduction

Communication : The process of sending information from one place to another place is called communication. The information maybe analog or digital information

Modulation : It is the process of changing the characteristic's of carrier signal according to the message signal.

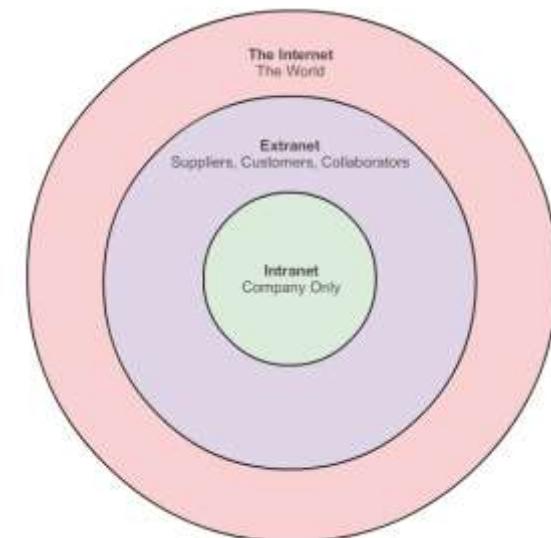
Need for modulation : It helps to transmit low frequency message signal to very large distance with the help of high frequency carrier signal

Introduction

Internet : The Internet is a **vast network that connects computers all over the world.** Through the Internet, people can share information and communicate from anywhere with an Internet connection.

Intranet : An intranet is a computer network for sharing information **within an organization**, usually to the exclusion of access by outsiders.

Extranet : **Suppliers, Customers, Collaborators.**



Introduction

Basic Components of Computer Networks :

- Message
- Sender
- Receiver
- Transmission Media
- Protocols

Introduction

Basic Features of Computer network:

- Communication Speed
- File Sharing
- Software and Hardware is Sharing
- Security
- Scalability
- Reliability

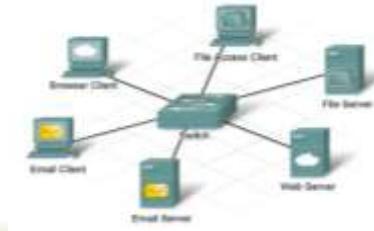
Introduction

Computer Network Architecture:

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

Two types of network architectures are used:

- Peer-To-Peer network
- Client/Server network



Introduction

Computer Network Architecture:

- **Peer-To-Peer network :** is a network in which all the computers are linked together with equal privilege and responsibilities for processing the data.
- Peer-To-Peer network is useful for small environments, usually up to 10 computers.
- Peer-To-Peer network has no dedicated server.

Advantages

- ❖ It is less costly as it does not contain any dedicated server.
- ❖ If one computer stops working , other computers will not stop working.
- ❖ It is easy to set up and maintain as each computer manages itself.

Disadvantages

- ❖ In the case of Peer-To-Peer network, it does not contain the centralized system . Therefore, it cannot back up the data as the data is different in different locations.
- ❖ It has a security issue as the device is managed itself.

Introduction

Computer Network Architecture:

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

Introduction

Computer Network Architecture:

Advantages

- ❖ A Client/Server network contains the centralized system. Therefore we can back up the data easily.
- ❖ A Client/Server network has a dedicated server that improves the overall performance of the whole system.
- ❖ Security is better in Client/Server network as a single server administers the shared resources.

Disadvantages

- ❖ Client/Server network is expensive as it requires the server with large memory.
- ❖ It requires a dedicated network administrator to manage all the resources.

Introduction

Computer Network Types :

A computer network can be categorized by their size and type.
A **computer network** is mainly classified as:

- LAN (Local Area Network)
- PAN (Personal Area Network)
- MAN (Metropolitan Area Network)
- WAN (Wide Area Network)
- SAN (Storage Area Network)

Introduction

LAN (Local Area Network):

- Local Area Network is a group of computers connected to each other in a small area such as building, office.
- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
- It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables.
- The data is transferred at an extremely faster rate in Local Area Network.
- Local Area Network provides higher security.

Introduction

PAN (Personal Area Network):

- Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.
- Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network.
- Personal computer devices that are used to develop the personal area network are the laptop, mobile phones, media player and play stations.
- Personal Area Network covers an area of 30 feet.



Introduction

MAN (Metropolitan Area Network):

- A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
- Government agencies use MAN to connect to the citizens and private industries.
- In MAN, various LANs are connected to each other through a telephone exchange line.
- It has a higher range than Local Area Network(LAN).

Examples:

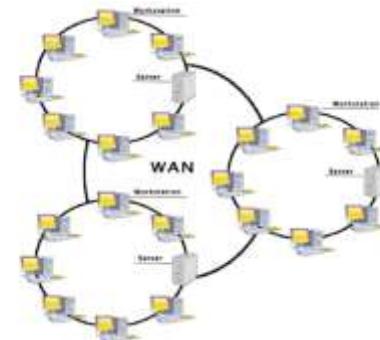
- ❖ MAN is used in communication between the banks in a city.
- ❖ It can be used in a college within a city.
- ❖ It can also be used for communication in the military.



Introduction

WAN (Wide Area Network):

- A Wide Area Network is a network that extends over a large geographical area such as states or countries.
- A Wide Area Network is widely used in the field of Business, government, and education.
- A Wide Area Network is quite bigger network than the LAN.
- A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fiber optic cable or satellite link
- The internet is one of the biggest WAN in the world.



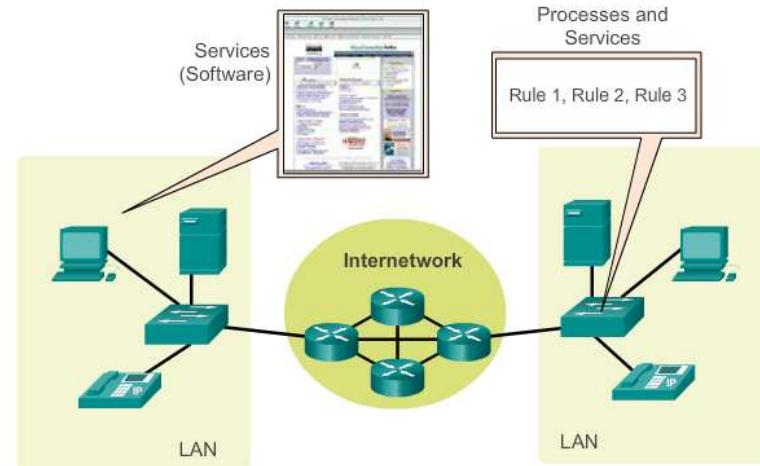
Network Hardware

What are network devices?

Network devices, or networking hardware, are physical devices that are required for communication and interaction between hardware on a computer Network.

There are three categories of network components:

1. Devices
2. Services
3. Media



Network Hardware

1. Devices :

Intermediary Devices :

- Hub
- Switch
- Router
- Bridge
- Modem
- Repeater
- Access Point
- NIC
- Firewall

End Devices :

- Computers (work stations, laptops, file servers, web servers)
- Network printers
- Phones
- Security cameras
- Mobile handheld devices (such as smart phones, tablets, and barcode scanners)

Network Hardware

Intermediary Devices : NIC

- NIC is used physically to connect host devices to the network media.
- A NIC is a printed circuit board that fits into the expansion slot of a bus on a computer motherboard.
- NICs are sometimes called network adapters.
- Each NIC is identified by a unique code called a Media Access Control (MAC) address.
- This address is used to control data communication for the host on the network.



Network Hardware

Intermediary Devices : Repeaters

- A repeater is a network device used to regenerate a signal.
- Repeaters regenerate analog or digital signals that are modified by transmission loss due to attenuation.
- A repeater does not make an intelligent decision like forwarding packets



Network Hardware

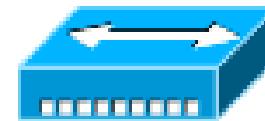
Intermediary Devices : HUB

100BaseT Hub

- Hubs concentrate on connections.
- In other words, they take a group of hosts and allow the network to see them as a single unit. This is done passively, without any other effect on the data transmission.



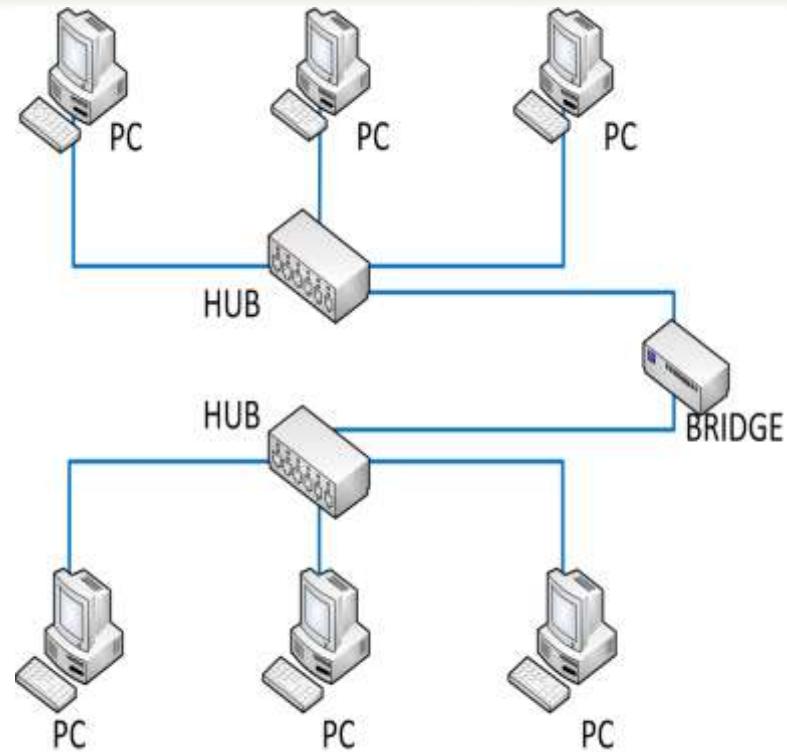
10BaseT Hub



Network Hardware

Intermediary Devices : Bridge

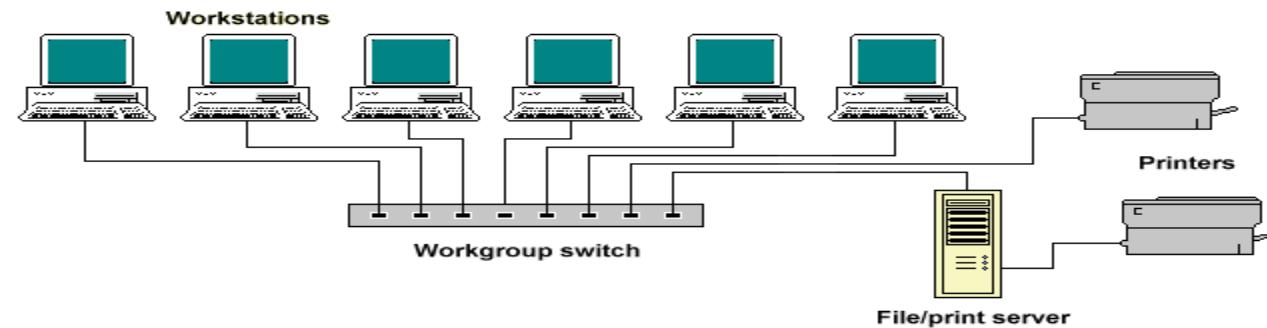
- Bridges provide connections between LANs.



Network Hardware

Intermediary Devices : Switches

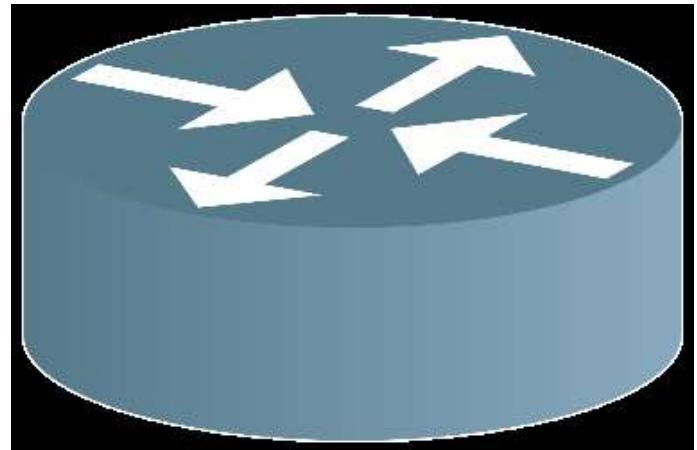
- Switches add more intelligence to data transfer management.
- They can determine if data should remain on a LAN and transfer data only to the connection that needs it.



Network Hardware

Intermediary Devices : Router

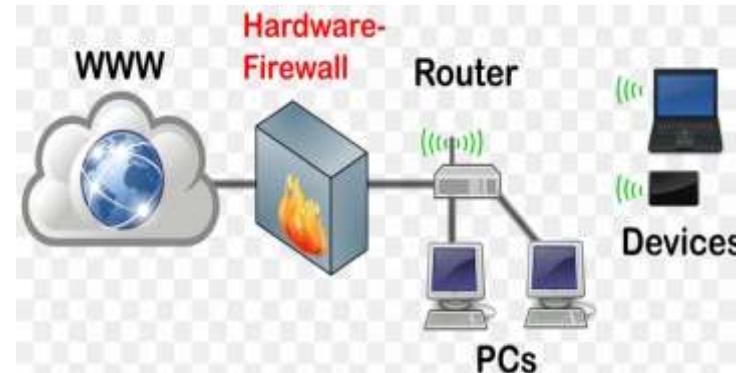
- Routers have all the capabilities listed above.
- Routers can regenerate signals, concentrate multiple connections, convert data transmission formats, and manage data transfers.
- They can also connect to a WAN, which allows them to connect LANs that are separated by great distances.



Network Hardware

Intermediary Devices : Firewall

- A firewall is a network device or software for controlling network security and access rules.
- Firewalls are inserted in connections between secure internal networks and potentially insecure external networks such as the Internet.
- Firewalls are typically configured to reject access requests from unrecognized sources while allowing actions from recognized ones.



Network Hardware

Intermediary Devices : Access Point

Network Hardware

Intermediary Devices : Modem

- A modem is a hardware device that allows the computer to connect to the internet over the existing telephone line.
- It stands for Modulator/Demodulator. It converts the digital data into an analog signal over the telephone lines.

Network Hardware

2. Services :

- **File Services**
 - ❖ File Sharing
 - ❖ File Transfer
- **Application Services**
 - ❖ Resource Sharing
 - ❖ Databases
 - ❖ Web Services
- **Communication Services**
 - ❖ Email
 - ❖ Social Networking
 - ❖ Internet Chat
 - ❖ Remote Access

Network Hardware

3. Network Media :

The function of the media is to carry a flow of information through a LAN.

A. Wired Media:- A widely adopted *family* that uses copper and fibre media in local area network (LAN) technology are collectively known as Ethernet

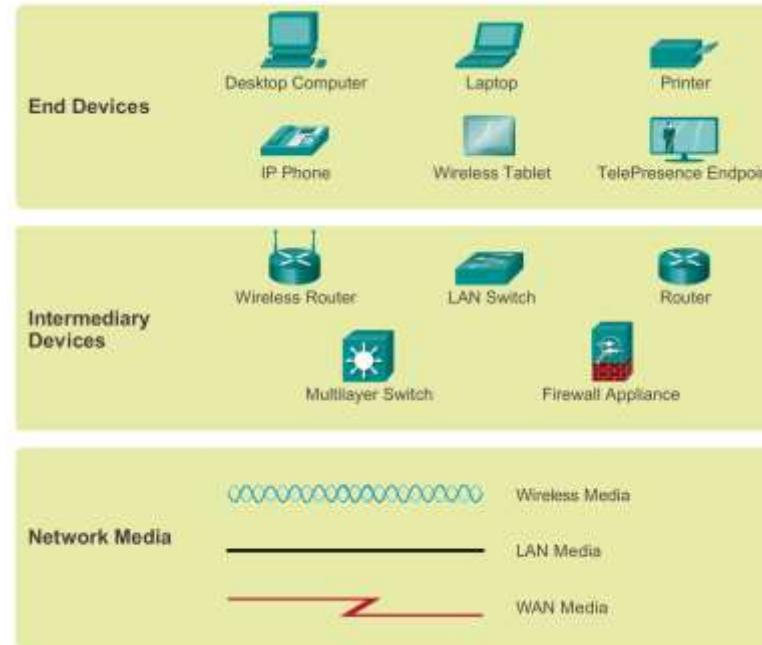
1. Copper Cable
 - a. Coaxial Cables
 - b. Shielded Twisted Pair(STP)
 - c. Unshielded Twisted Pair
2. Fibre Optic Cable

B. Wireless Media:- use the atmosphere, or space, as the medium.



Network Hardware

Network Representations :



Transmission Modes

There are three modes of transmission for data communication depending on the direction of transfer.

- Simplex
- Full-Duplex
- Half-Duplex

Network Software

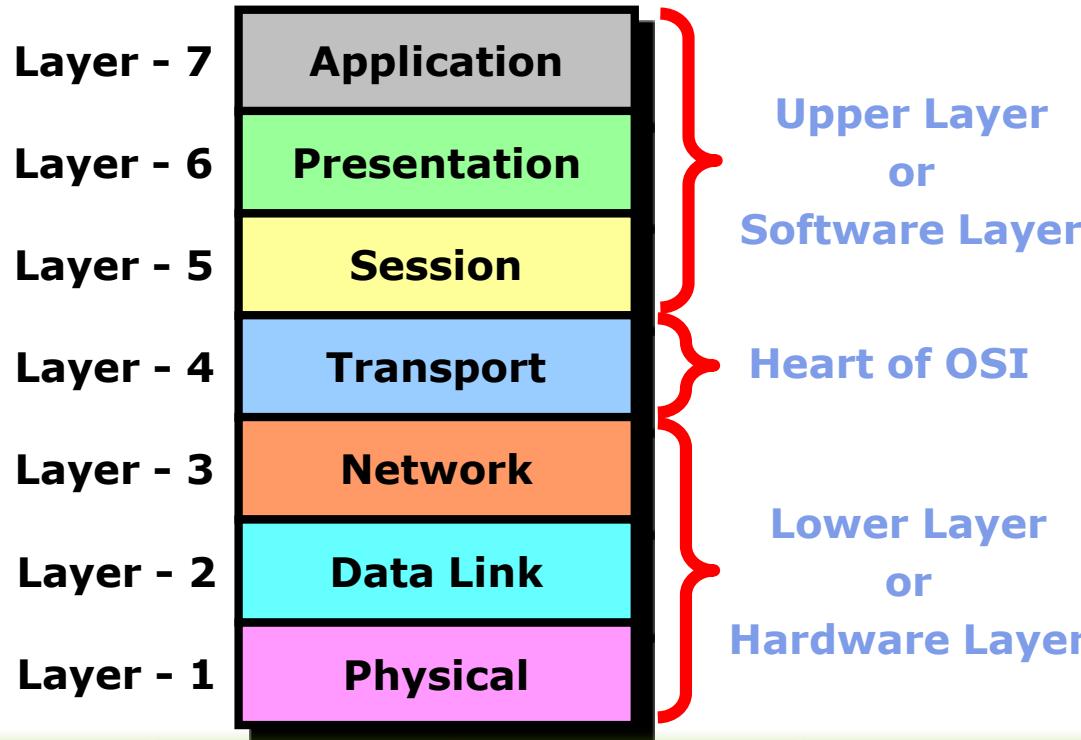
Reference Models

OSI : Open System Interconnect model

- OSI means Open System Interconnect model.
- Developed by the International Organization for Standardization in 1974.
- It consists of seven layers.
- Each layer has a different but specific processing function.

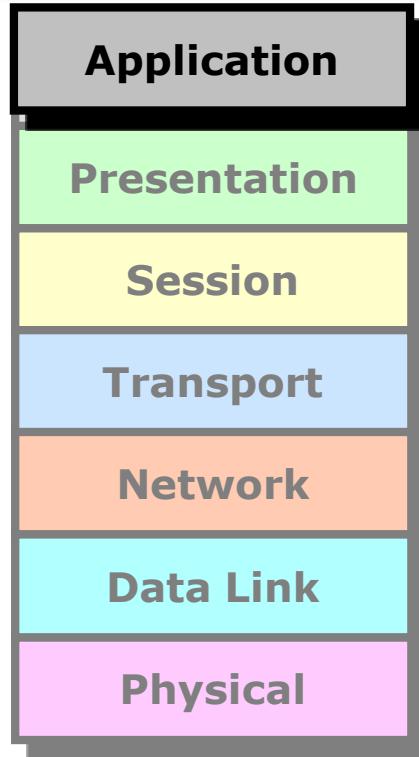
Reference Models

OSI : Open System Interconnect model



OSI Reference Models

Application Layer :



Application Layer is responsible for providing Networking Services to the user. It is also known as Desktop Layer. Identification of Services is done using Port Numbers.

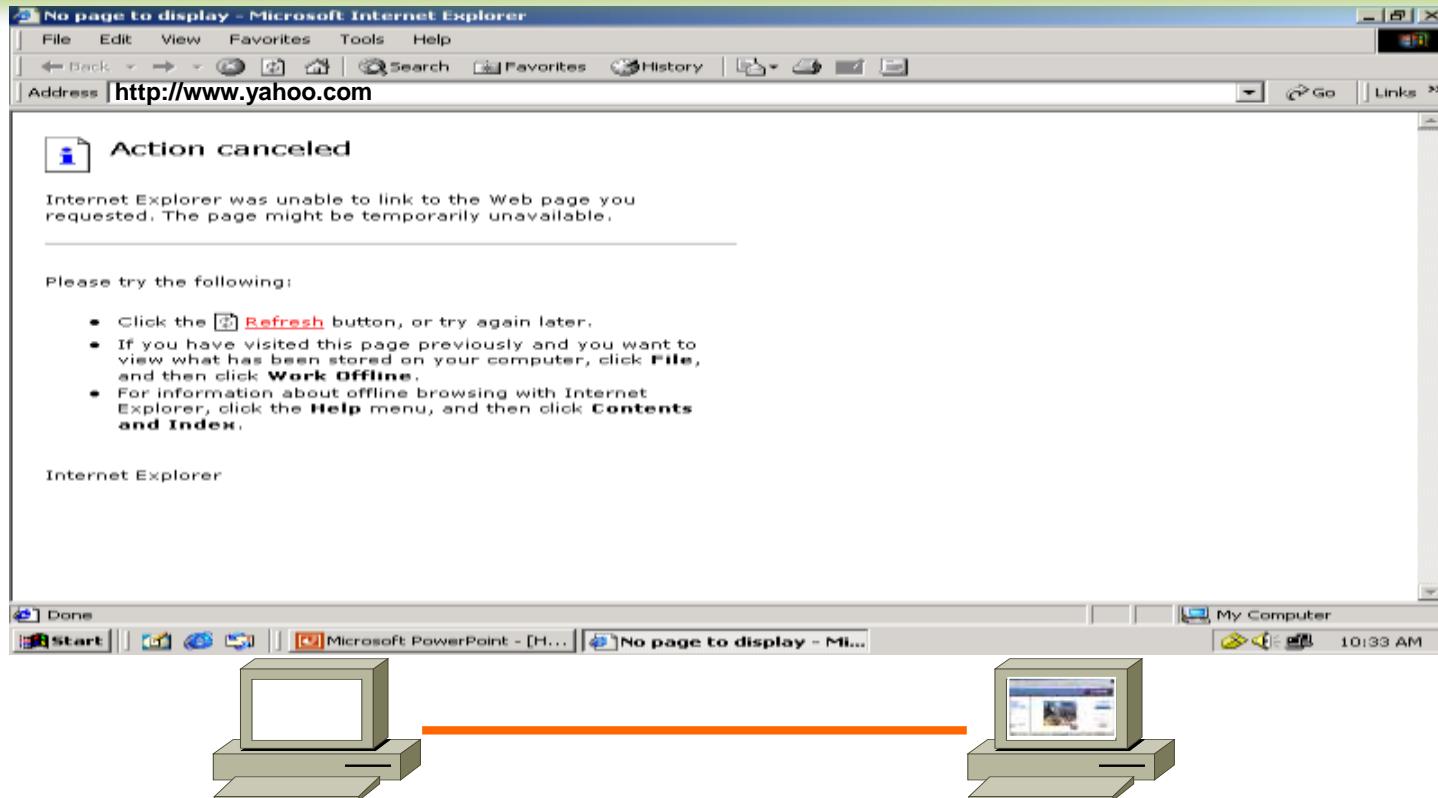
Ports are Entry and Exit Points to the Layer

Total No. Ports **0 – 65535**

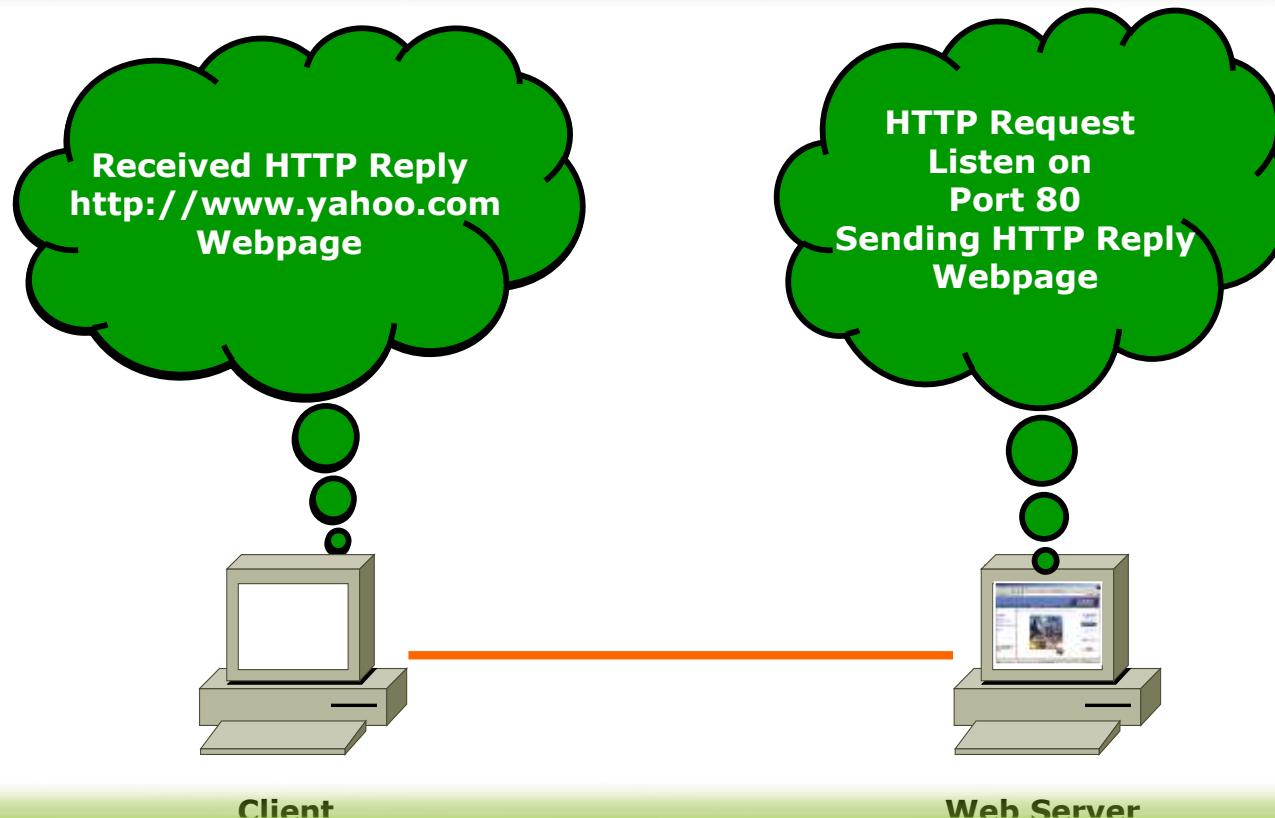
Reserved Ports **0 – 1023**

Open Client Ports **1024 – 65535**

Example of HTTP request

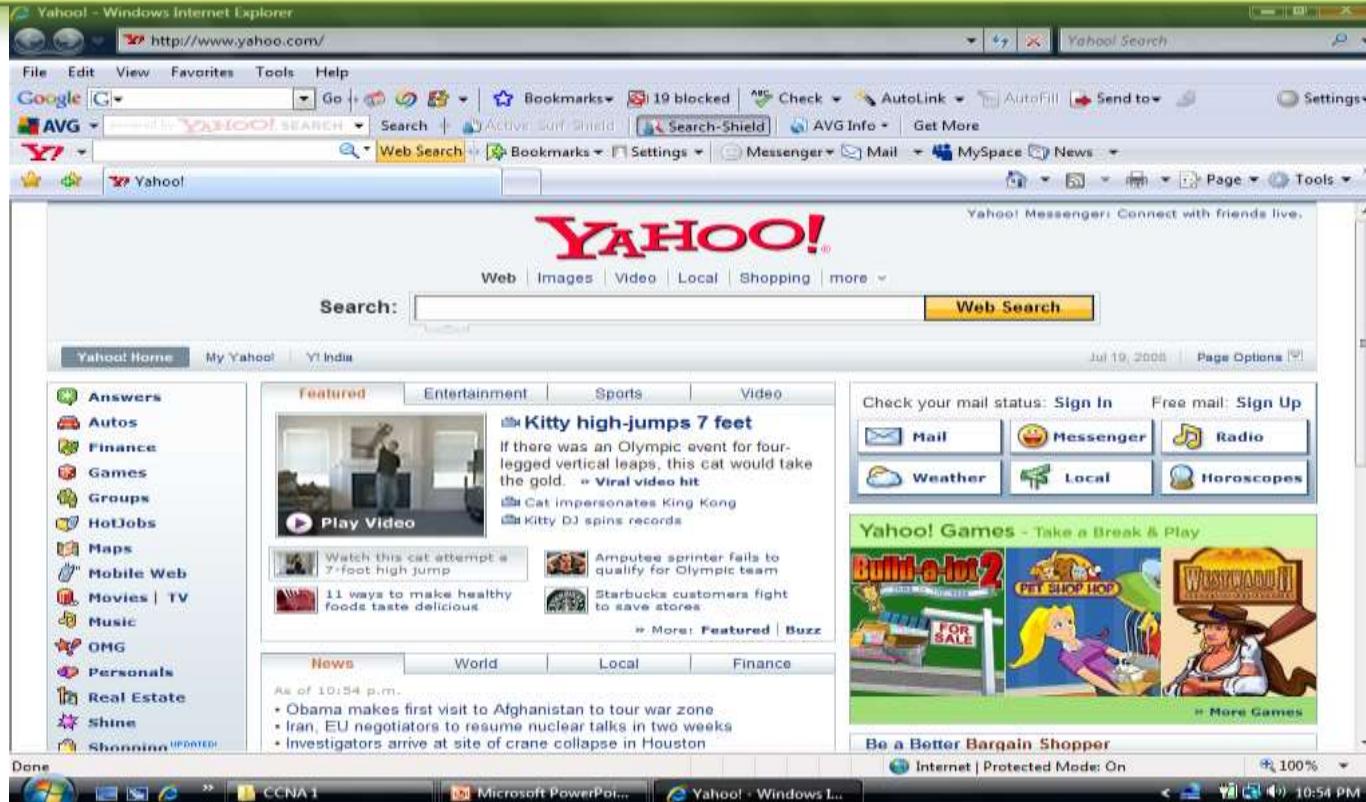


Example of HTTP request

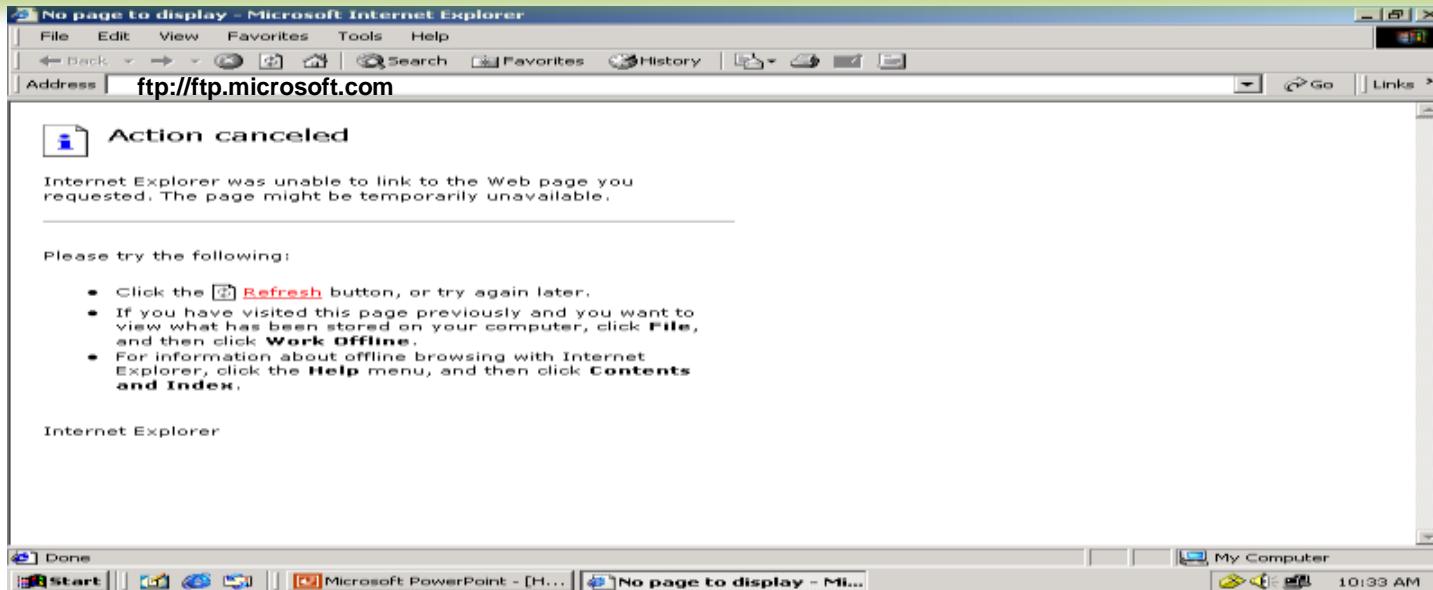


Client

Web Server



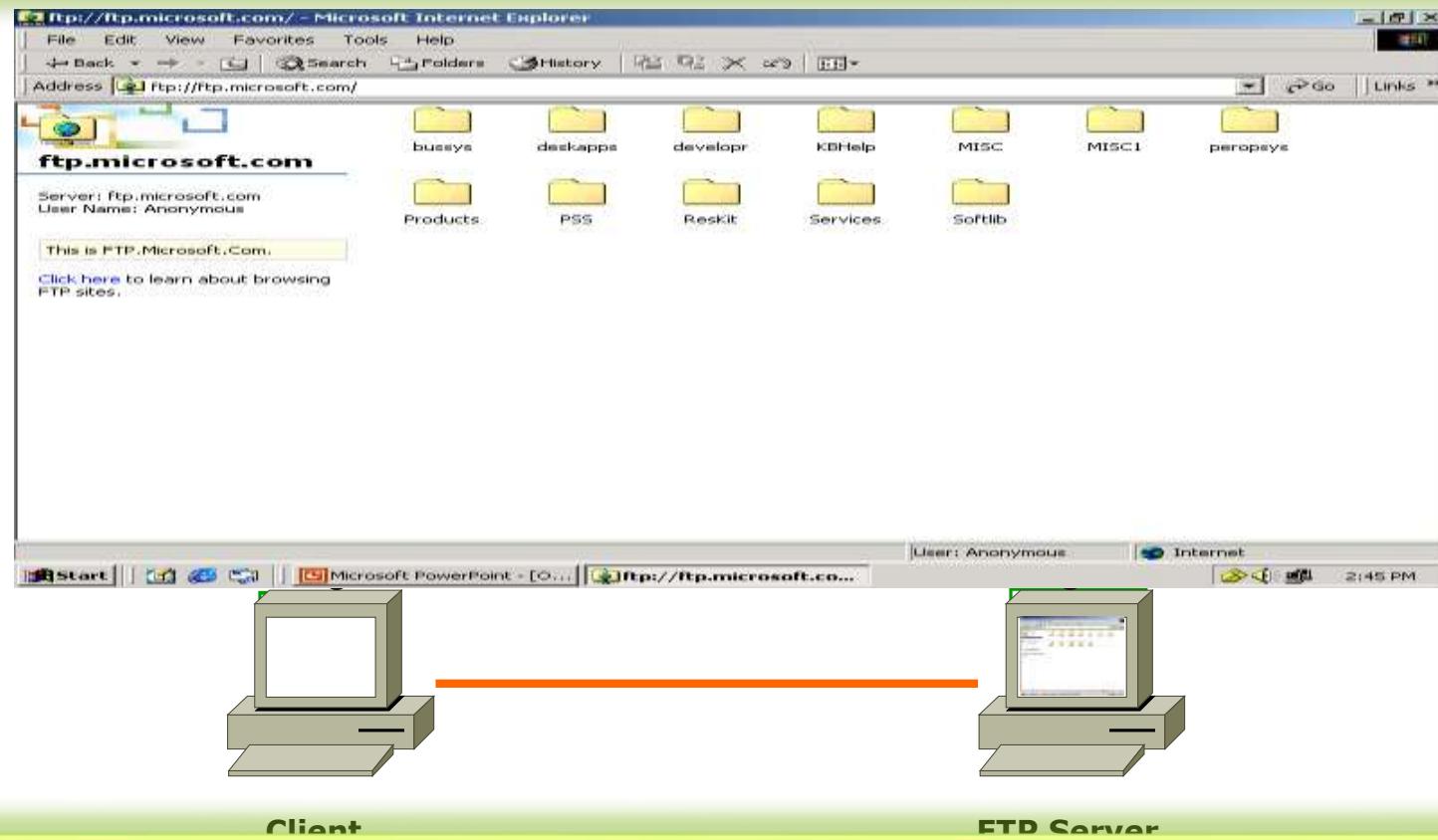
Example of FTP request



Client

FTP Server

Example of FTP request



Examples of Networking Services

Service Port No.

HTTP **80**



FTP **21**

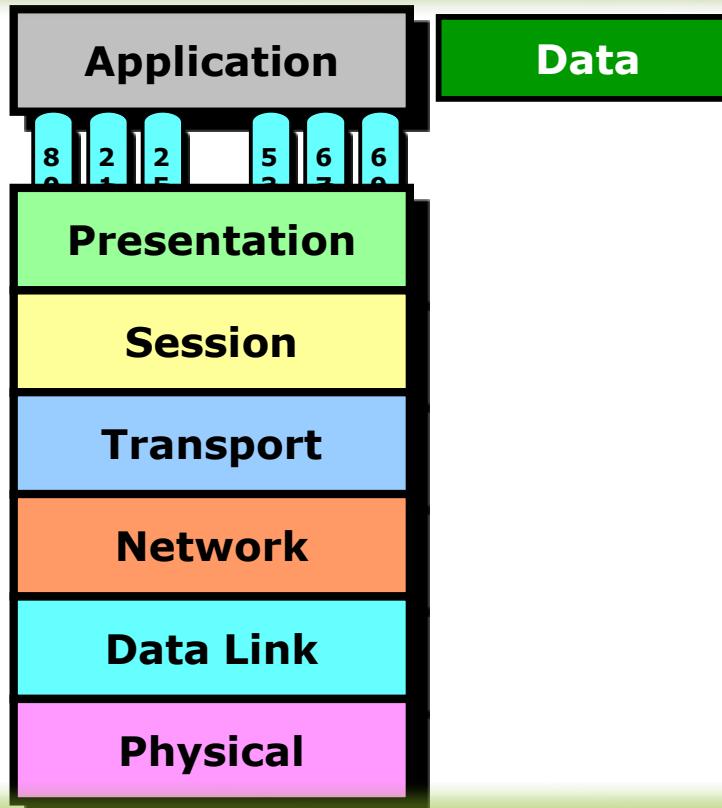


SMTP **25**

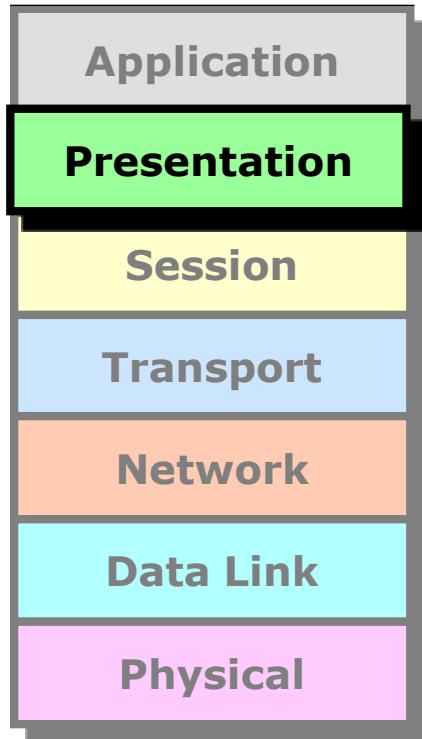
TELNET **23**



Data flow from Application Layer



Presentation Layer



Presentation Layer is responsible for converting data into standard format.

Examples : **ASCII, EBCDIC, JPEG, MPEG, BMP, MIDI, WAV, MP3**

Following tasks are perform at Presentation layer :

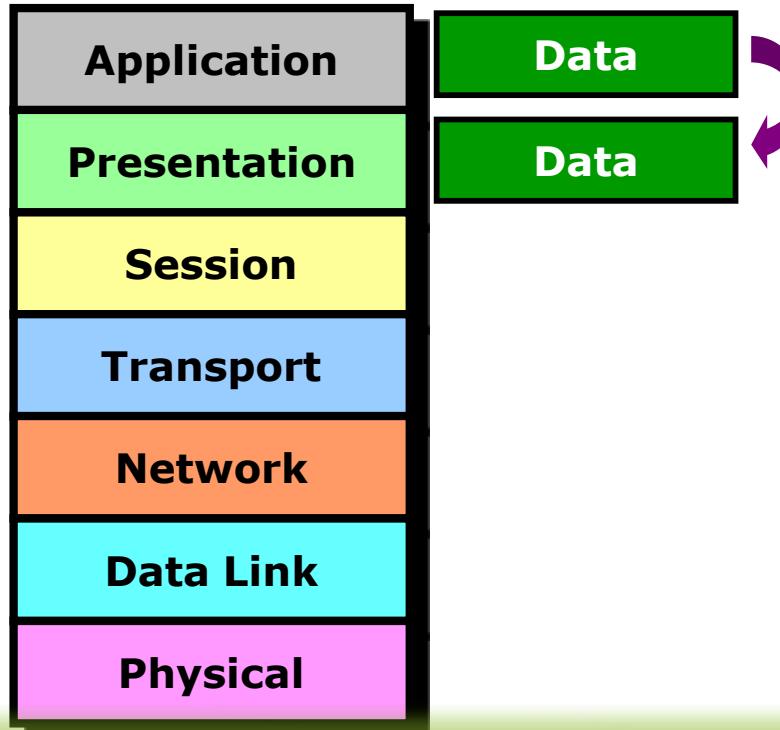


Encoding – Decoding

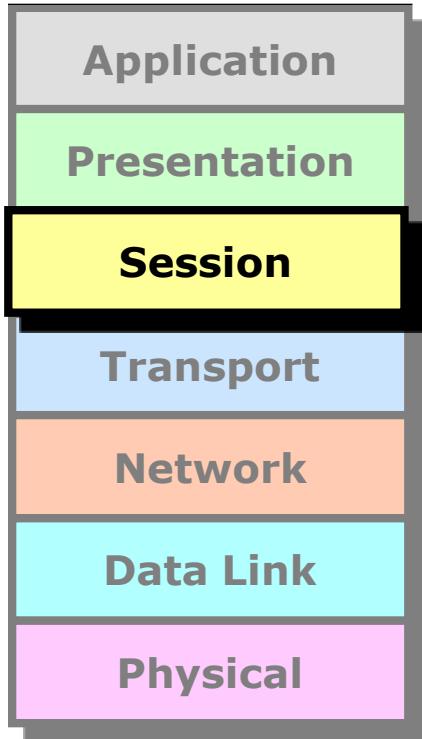
Encryption – Decryption

Compression – Decompression

Data flow from Presentation Layer



Session Layer



Session Layer is responsible for establishing, maintaining and terminating session.

Session ID works at Session Layer.

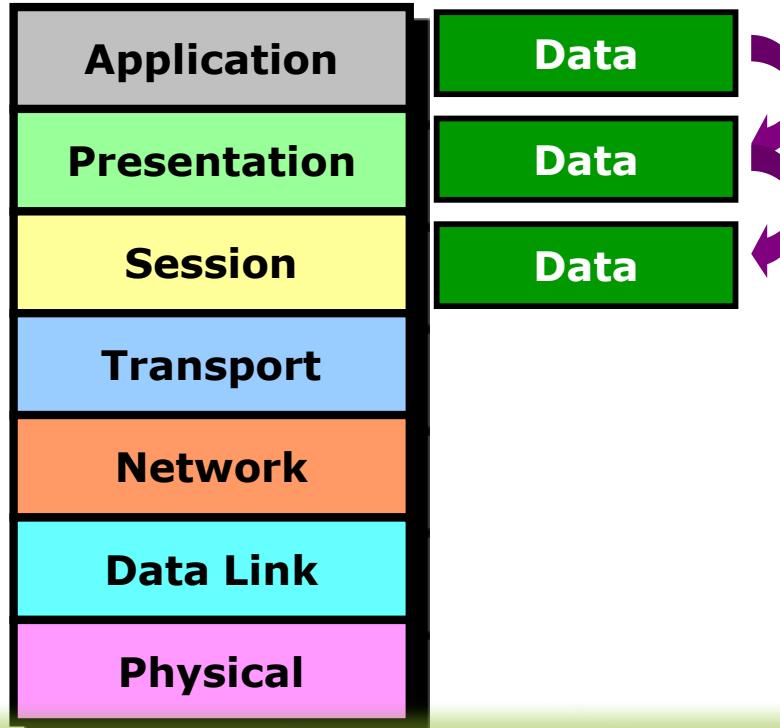


Examples :

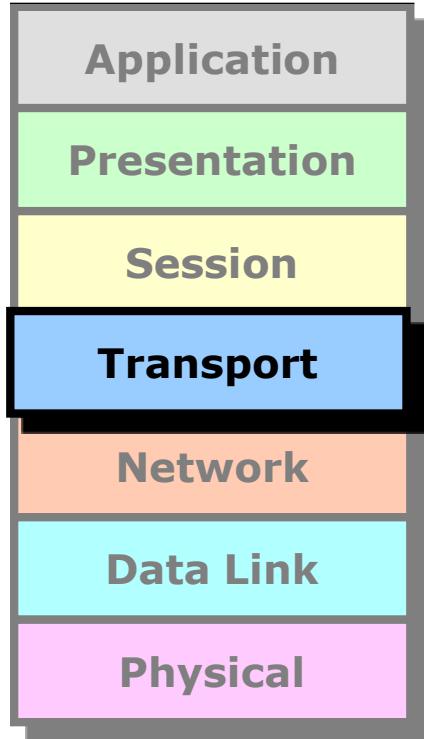
RPC → Remote Procedure Call

SQL → Structured Query Language

Data flow from Session Layer



Transport Layer



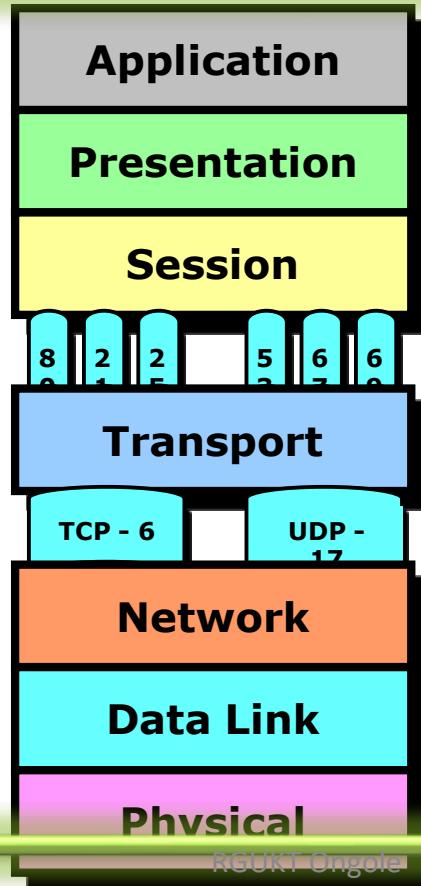
Transport Layer is responsible for end-to-end connectivity. It is also known as the heart of OSI Layers. Following tasks are performed at the Transport Layer : -

- Identifying Service
- Multiplexing & De-multiplexing
- Segmentation
- Sequencing & Reassembling
- Error Correction
- Flow Control

Identifying Service

TCP	UDP
<ul style="list-style-type: none">• Transmission Control Protocol• Connection Oriented• Acknowledgement• Reliable• Slower• Port No. 6• e.g. HTTP, FTP, SMTP	<ul style="list-style-type: none">• User Datagram Protocol• Connection Less• No Acknowledgement• Unreliable• Faster• Port No. 17• e.g. DNS, DHCP, TFTP

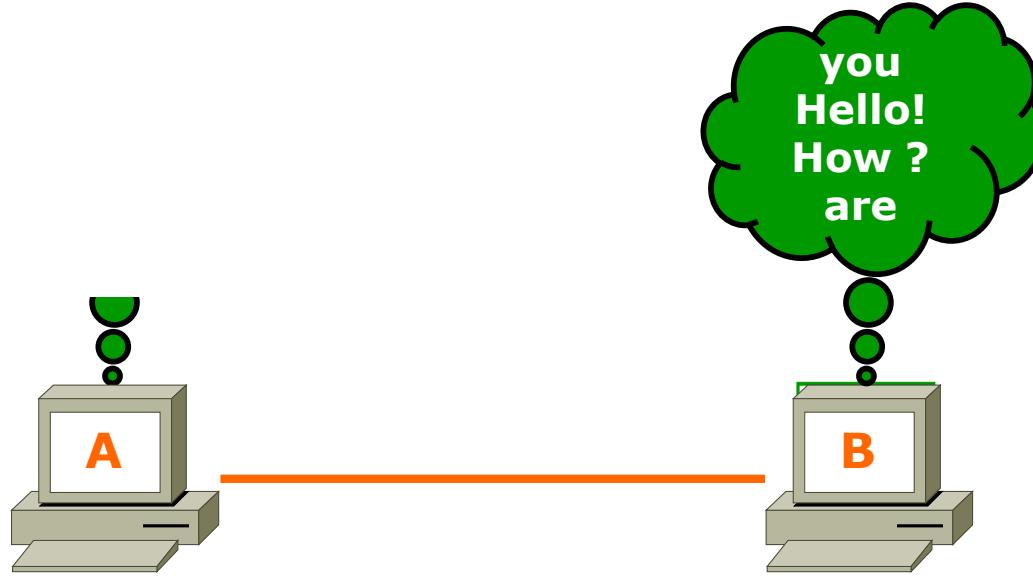
Multiplexing & De-multiplexing



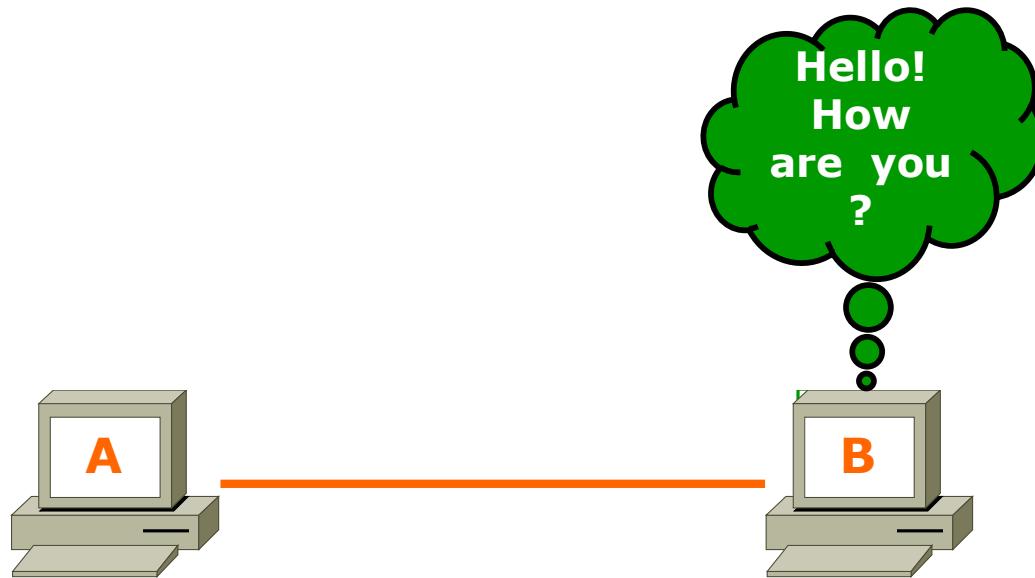
Segmentation



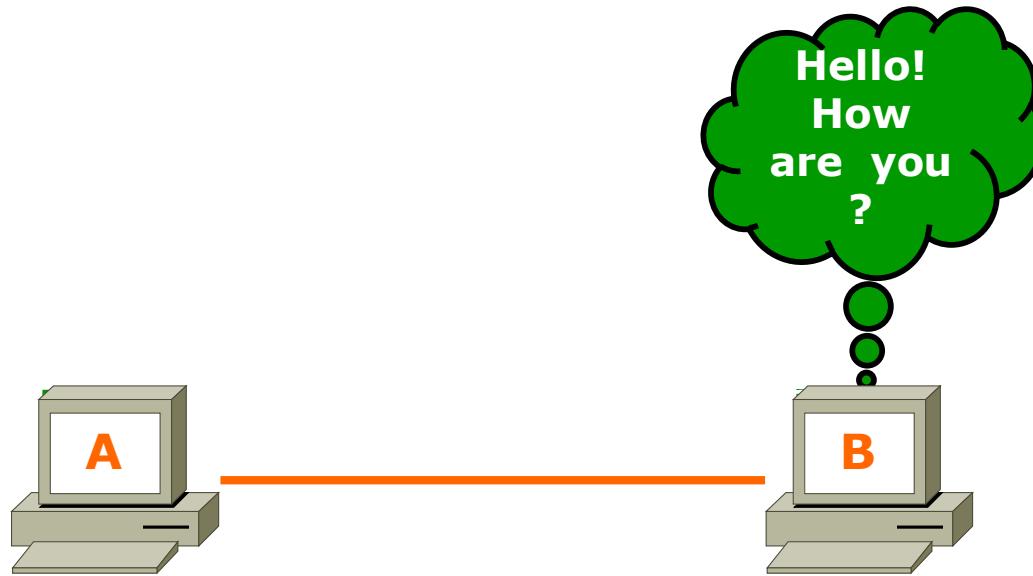
Sequencing & Reassembling



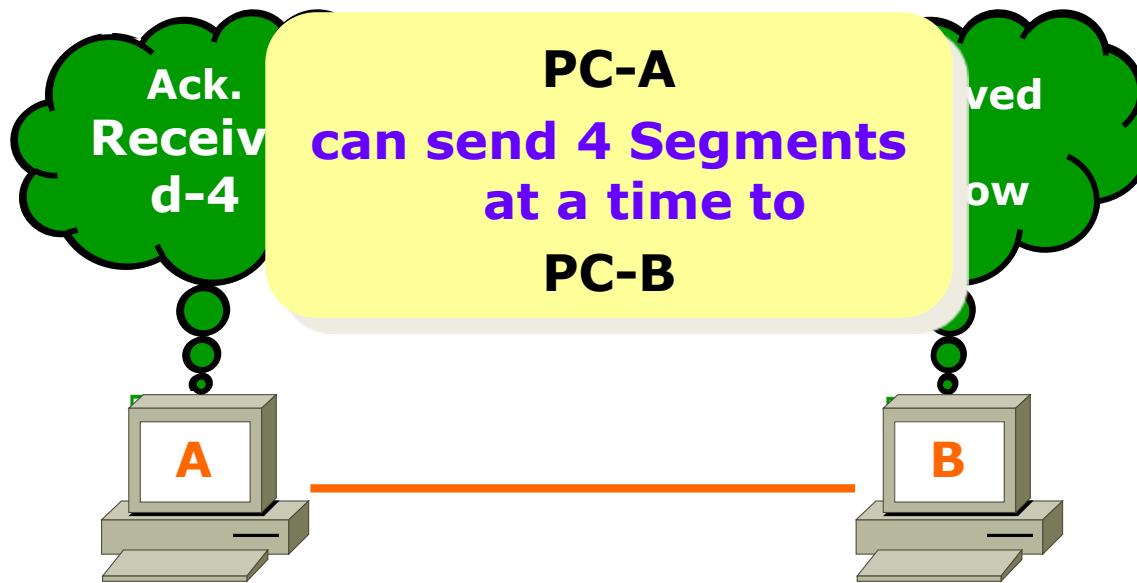
Sequencing & Reassembling



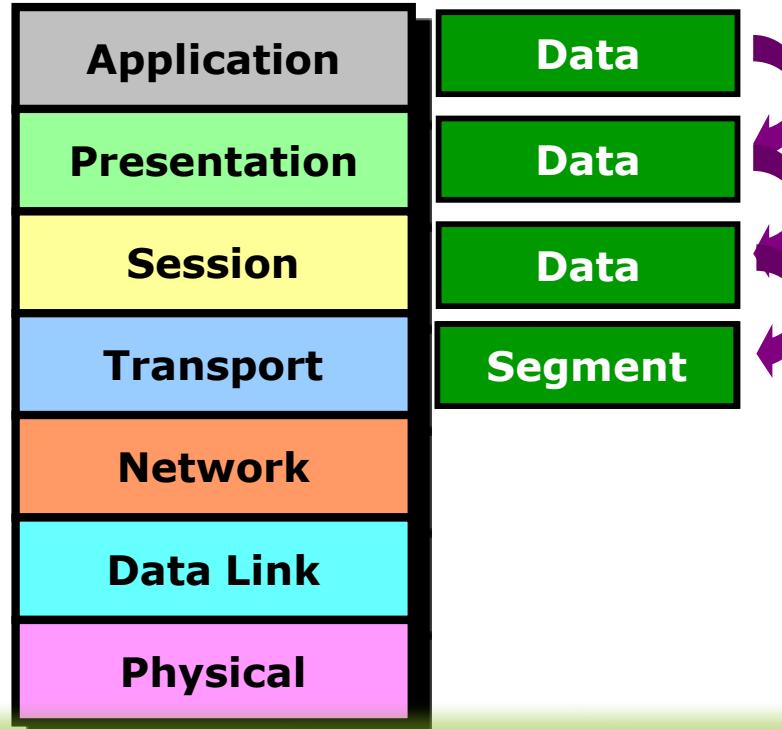
Error Correction



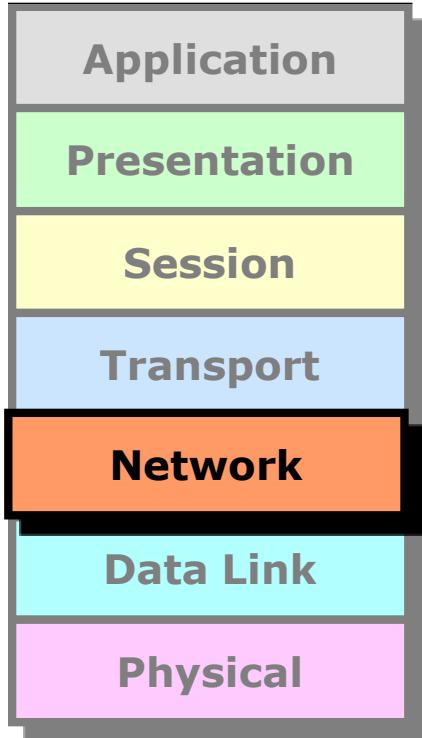
Flow Control - Windowing



Data flow from Transport Layer



Network Layer

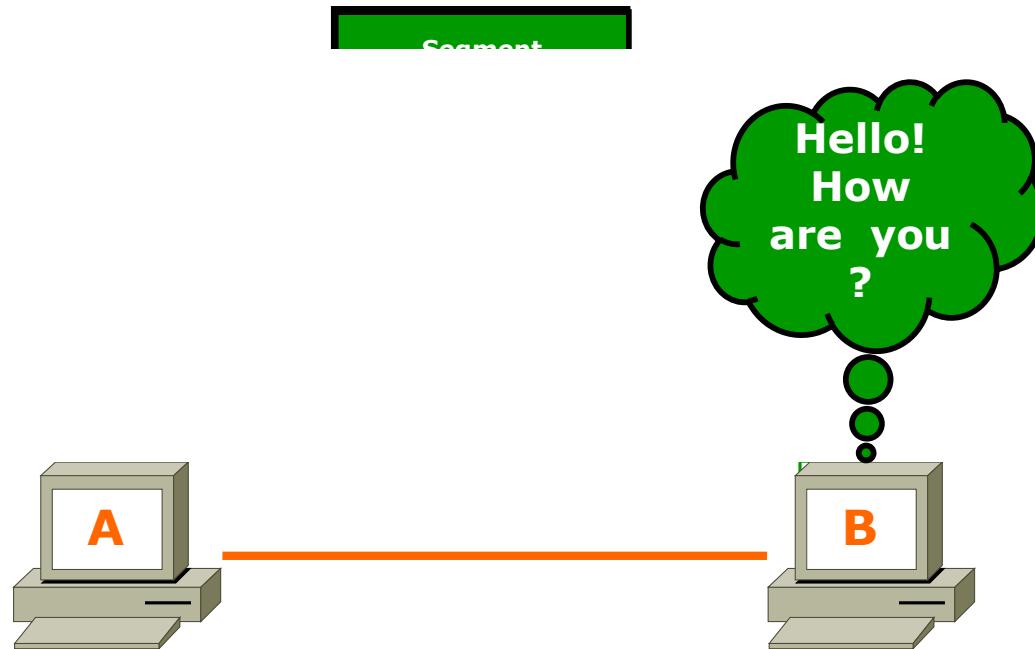


Network Layer is responsible for providing best path for data to reach the destination. Logical Addressing works on this layer. Router is a Network Layer device.

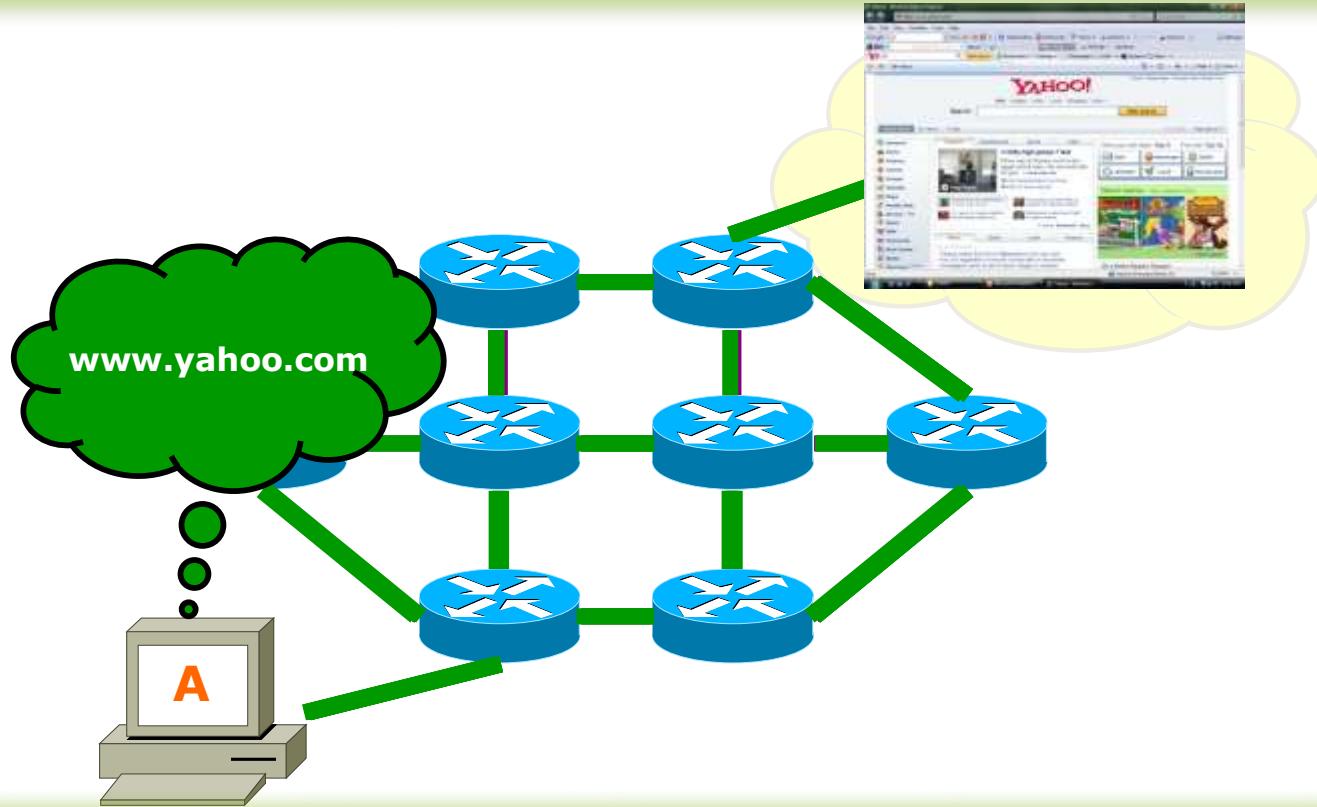
It is divided into two parts

- **Routed Protocols**
e.g. IP
- **Routing Protocols**
e.g. RIP, IGRP, OSPF, EIGRP

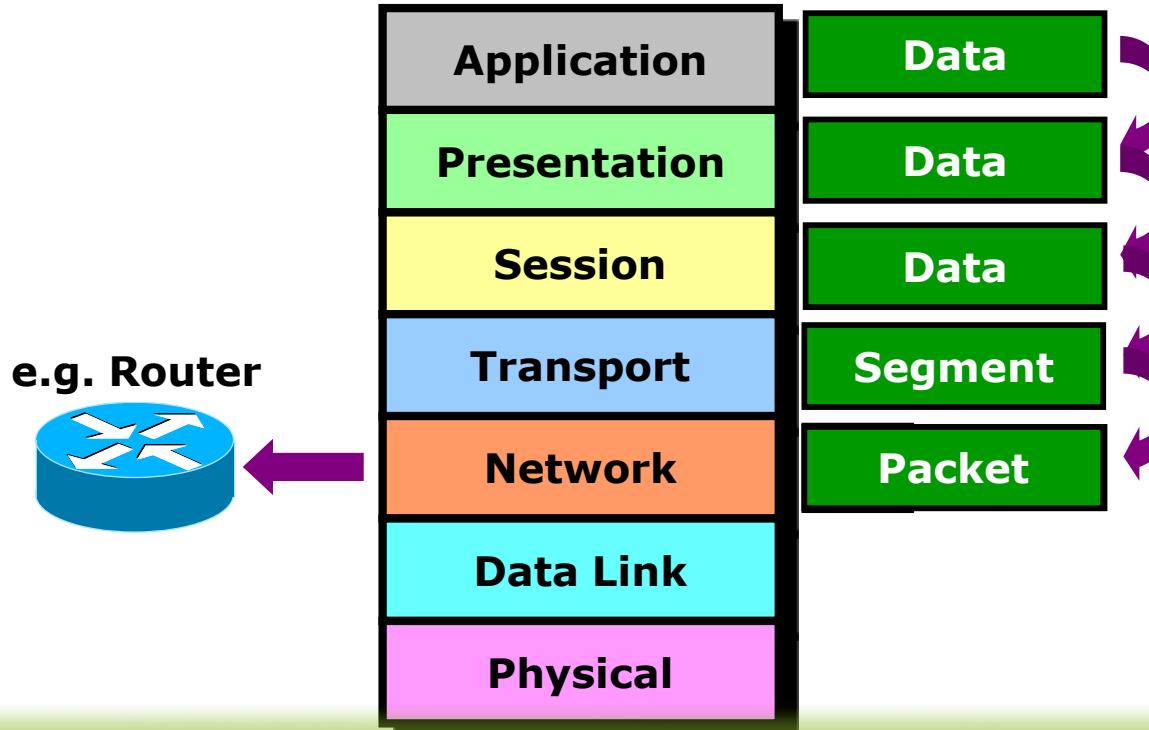
Routed Protocols



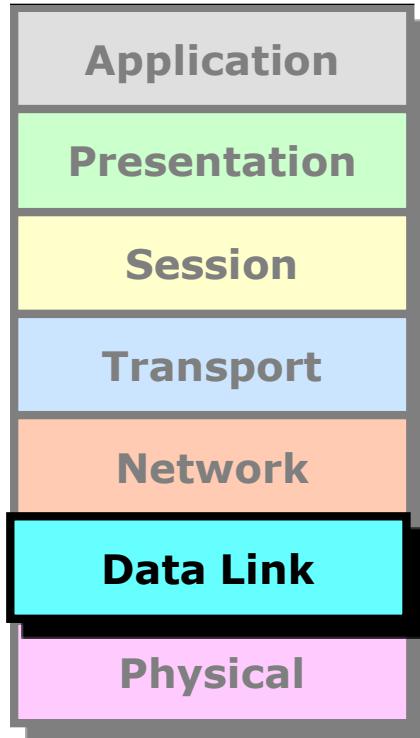
Routing Protocols



Data flow from Network Layer



Datalink Layer

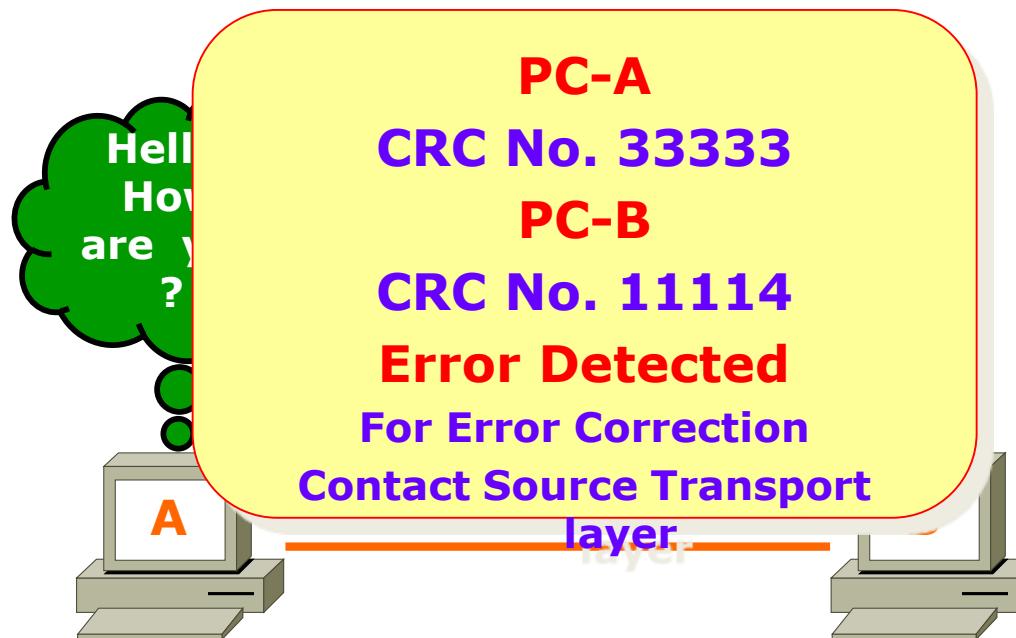


Datalink Layer is divided into two Sub Layers :

- **LLC – Logical Link Control**
It talks about Wan protocols
e.g. PPP, HDLC, Frame-relay
- **MAC – Media Access Control**
It talks about Physical Address. It is a 48 bit address i.e. 12 digit Hexadecimal Number.
It is also responsible for Error Detection

Devices working on Data Link Layer are Switch, Bridge, NIC.
RGHKT Ongole
CS3102 - COMPUTER NETWORKS

Error Detection – CRC Check



192.168.1.1

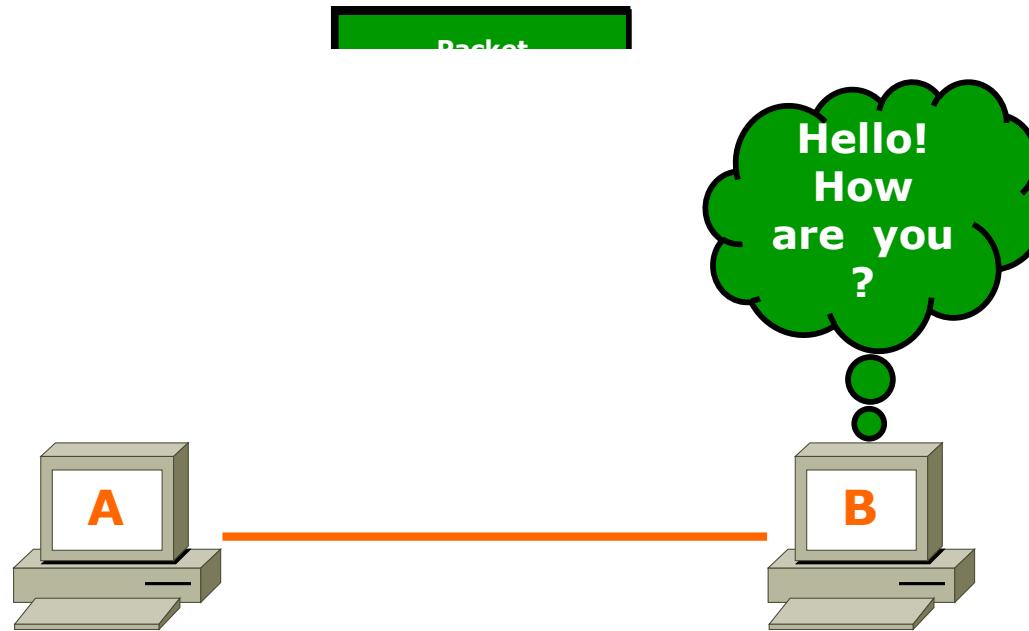
Mallikarjuna Nandi,
Assistant Professor
00-20-18-C0-07-71

192.168.1.2

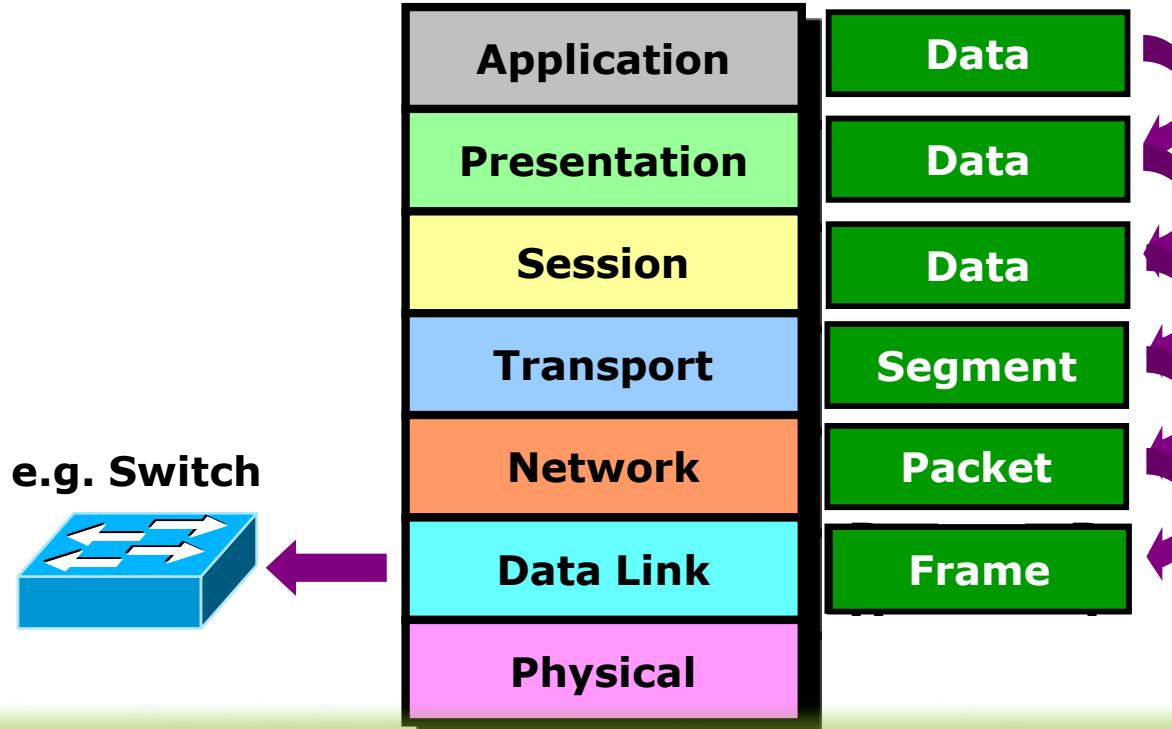
00-20-18-C0-07-72

RGUKT Ongole
CS3102 - COMPUTER NETWORKS

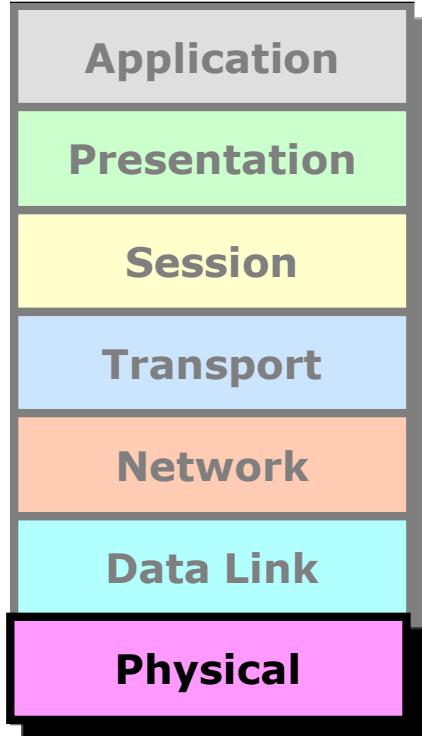
Error Detection – CRC Check



Data flow from Data Link Layer



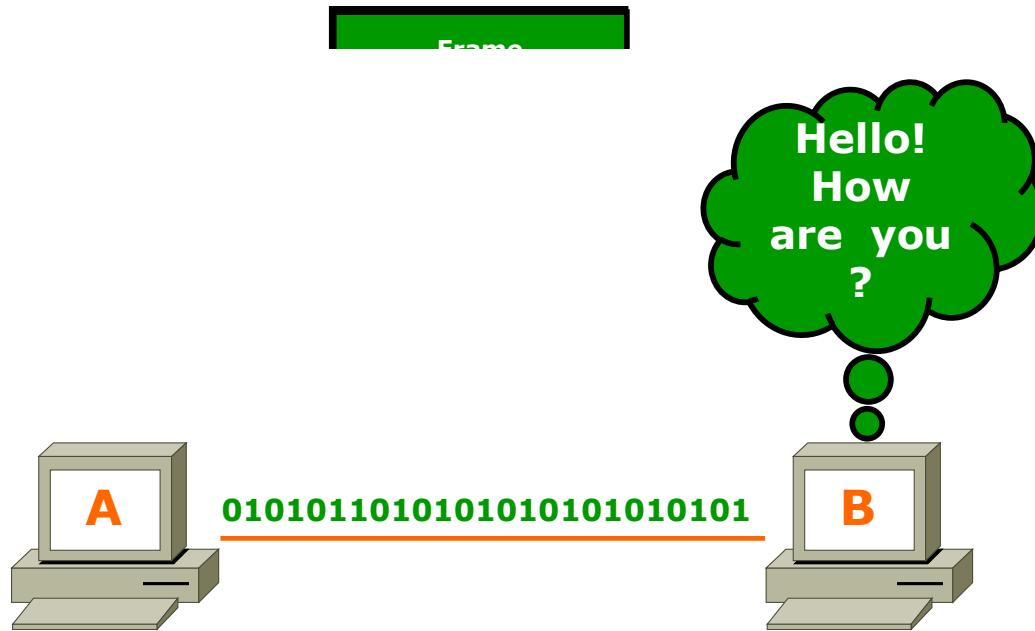
Physical Layer



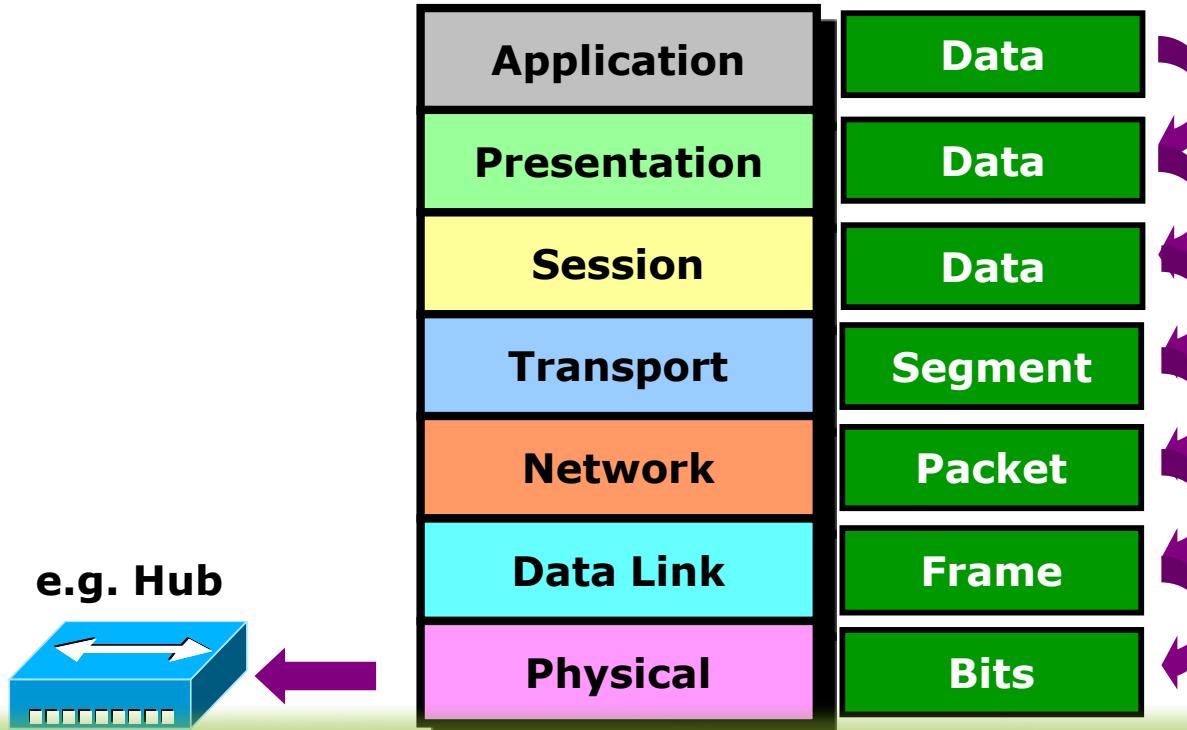
Physical Layer is responsible for electrical, mechanical and procedural checks. Data will be converted into Binary (i.e) 0's & 1's. Data will be in the form of electrical pulses if it is Coaxial or Twisted Pair cable and in the form of Light if it is Fiber Optic Cable.

Devices working at Physical Layer are Hubs, Repeaters, Cables, Modems etc.

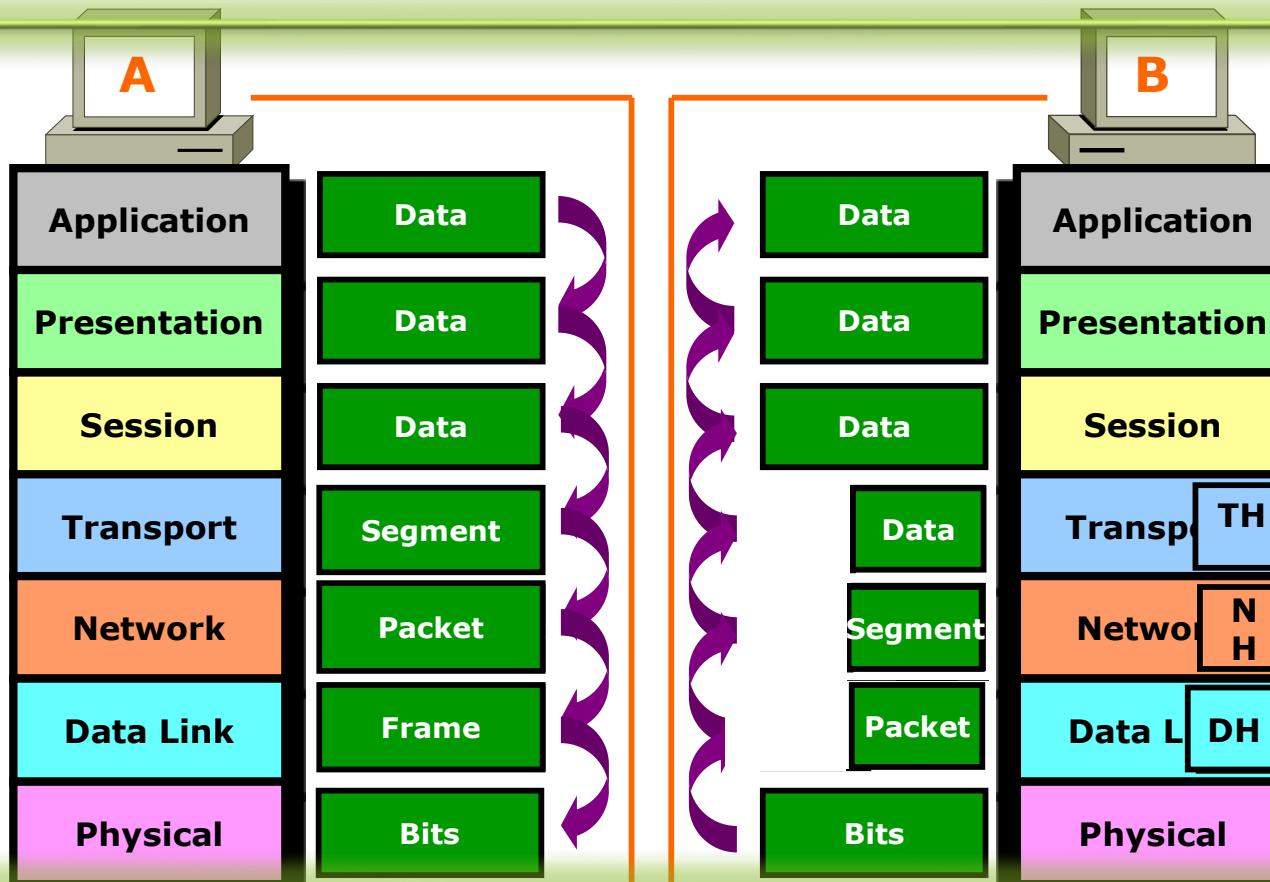
Physical Layer Example



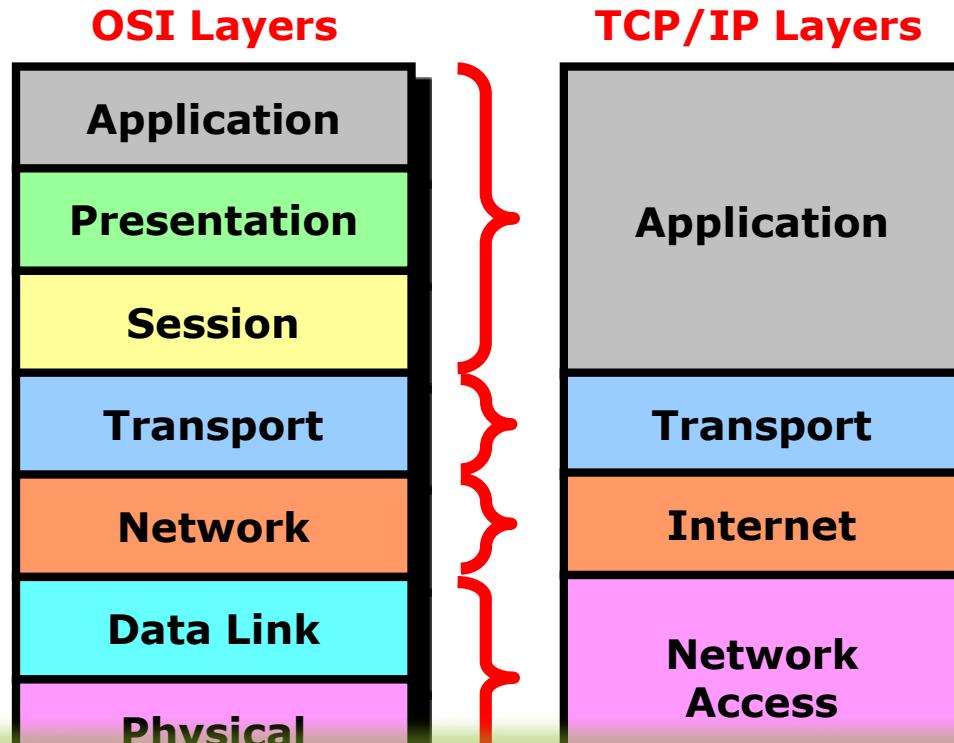
Data flow from Physical Layer



Data Encapsulation & De-capsulation



Comparing OSI with TCP/IP Layers



Network Topologies

Network topology defines the structure of the network.

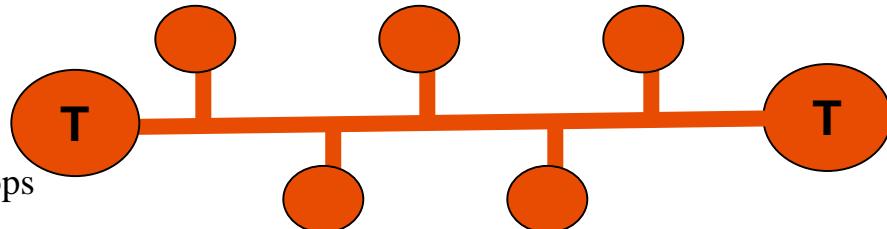
A. Physical topology:- It define the actual layout of the wire or media.

1. Bus
2. Ring
3. Star
4. Tree(Hierarchical)
5. Mesh
6. Hybrid Topology

Network Topologies

1. Bus Topology

All devices are connected to a central cable, called bus or backbone.



There are terminators at each end of the bus that stops the signal and keeps it from traveling backwards.

Advantages:

1. There is no central controller.
2. Control resides in each station
3. Less interconnecting wire is required.
4. Ease of installation.
5. Backbone cable can be laid along the most efficient path, and then connected to the nodes by drop lines of various lengths

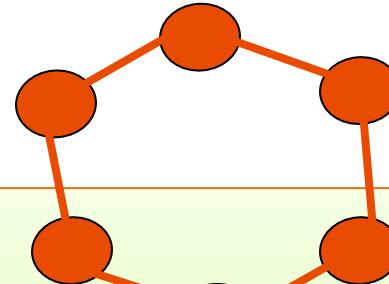
Disadvantages:

1. It is possible that more than one station may attempt transmission simultaneously (collision or contention).
2. Difficult reconfiguration and fault isolation.
3. A fault or break in the bus cable stops all transmission, even between devices on the same side of the problem.
4. The damaged area reflects signals in the direction of origin, creating noise in both directions

Network Topologies

2. Ring Topology

- All devices are connected to one another in the shape of a closed loop.
- Each device is connected directly to two other devices, one on either side of it.



Advantages:

1. Avoids the collisions that are possible in the bus topology.
2. Each pair of stations has a point-to-point connection.
3. A signal is passed along the ring in one direction, from device to another, until it reaches its destination.
4. Each device incorporates a repeater.
5. Relatively easy to install and reconfigure.
6. Fault isolation is simplified.

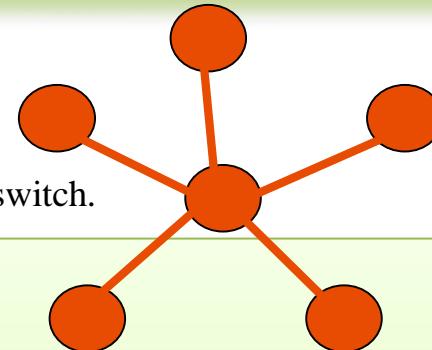
Disadvantages:

1. A break in the ring (such as station disabled) can disable the entire network.
2. Unidirectional traffic.

Network Topologies

3. Star Topology

- All devices are connected to a central hub.
- Nodes communicate across the network by passing data through the hub or switch.



Advantages:

1. Easy to install and reconfigure.
2. Robustness, if one link fails; only that link is affected. All other links remain active.
3. Easy fault identification and isolation. As long as the hub is working, it can be used to monitor link problems and bypass defective links.

Disadvantages:

1. The devices are not linked to each other.
2. If one device wants to send data to another, it sends it to the controller, which then relays the data to the other connected device.

Network Topologies

4. Tree/Hierarchical Topology

Advantages:

1. It allows more devices to be attached to a single central hub and can therefore increase the distance a signal can travel between devices.
2. It allows the network to isolate and prioritize communications from different computers.

Disadvantages:

1. The devices are not linked to each other.
2. If one device wants to send data to another, it sends it to the controller, which then relays the data to the other connected device.
3. The addition of secondary hubs brings two further advantages.



Network Topologies

4. Mesh Topology

Each host has its connections to all other hosts.

Mesh topology is implemented to provide as much protection as possible from interruption of service.

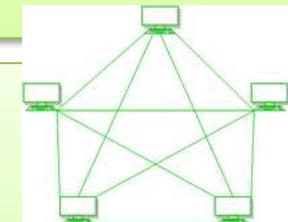
1. A nuclear power plant might use a mesh topology in the networked control systems.
2. Although the Internet has multiple paths to any one location, it does not adopt the full mesh topology.

Advantages:

1. The use of dedicated links guarantees that each connection can carry its data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.
2. It is robust, if one link becomes unusable, it does not incapacitate (affect) the entire system.
3. Privacy and Security (every message sent travels along a dedicated line; only the intended recipient sees it).
4. Point-to-point links make fault identification and fault isolation easy.

Disadvantages:

1. A large amount of cabling required.
2. A large amount of I/O ports required.
3. Installation and reconfiguration are difficult.
4. The sheer bulk of the wiring can be greater than the available space (in the walls, ceiling, or floors) can accommodate.
5. The hardware required to connect each link (I/O ports and cables) can be prohibitively expensive.



Physical Layer

Transmission Media :

The media over which the information between two computer systems is sent, called transmission media. Transmission media comes in two forms.

Guided Media : All communication wires/cables are guided media, such as UTP, coaxial cables, and fiber Optics. In this media, the sender and receiver are directly connected and the information is send (guided) through it.

Unguided Media :Wireless or open air space is said to be unguided media, because there is no connectivity between the sender and receiver. Information is spread over the air, and anyone including the actual recipient may collect the information.

Physical Layer

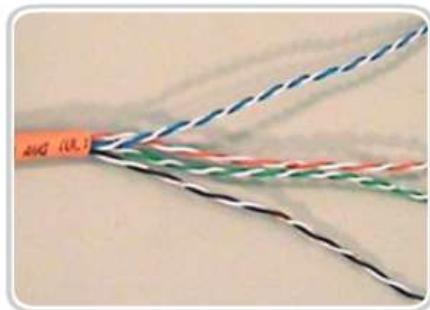
Channel Capacity

The speed of transmission of information is said to be the channel capacity. We count it as data rate in digital world. It depends on numerous factors such as:

- ❖ Bandwidth: The physical limitation of underlying media.
- ❖ Error-rate: Incorrect reception of information because of noise.
- ❖ Encoding: The number of levels used for signaling.

Physical Layer

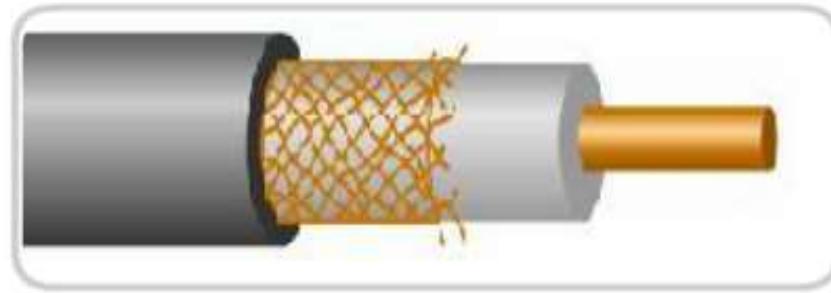
➤ **Copper Cable :** The most common, easiest, quickest, and cheapest form of network media to install. The disadvantage of sending data over copper wire is that the further the signal travels, the weaker it becomes.



Unshielded Twisted
Pair (UTP) Cable



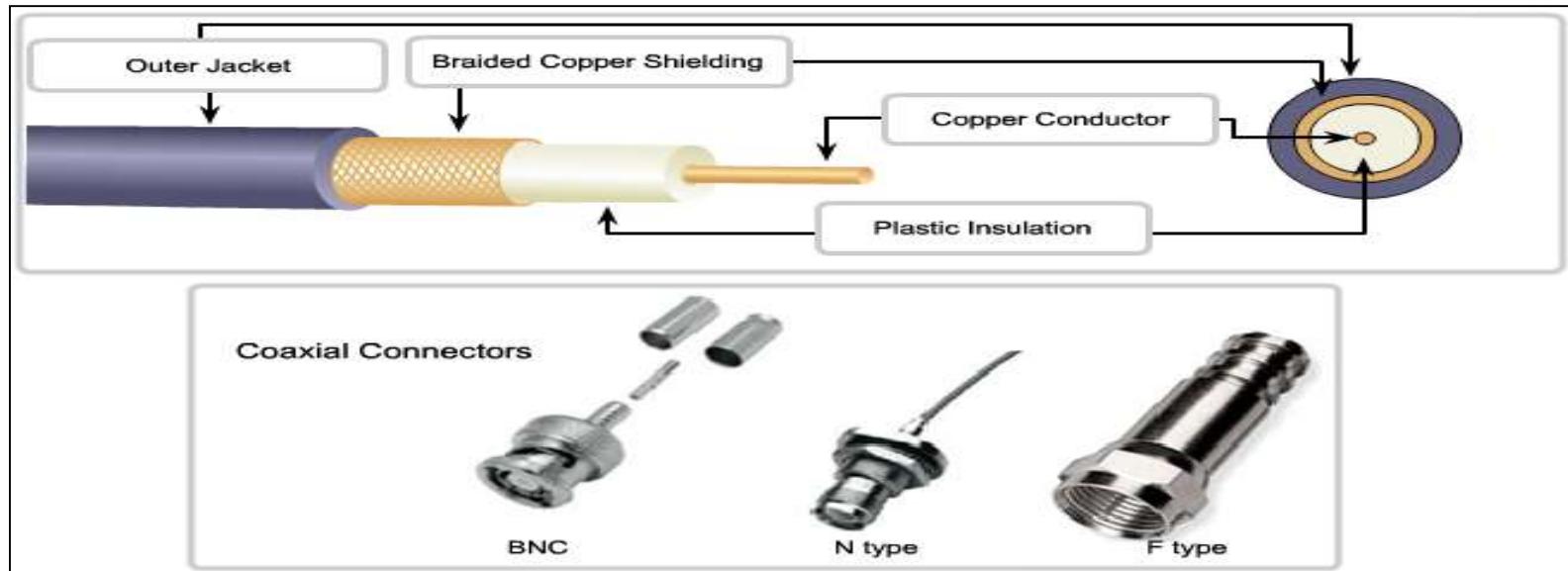
Shielded Twisted Pair
(STP) Cable



Coaxial Cable

Physical Layer

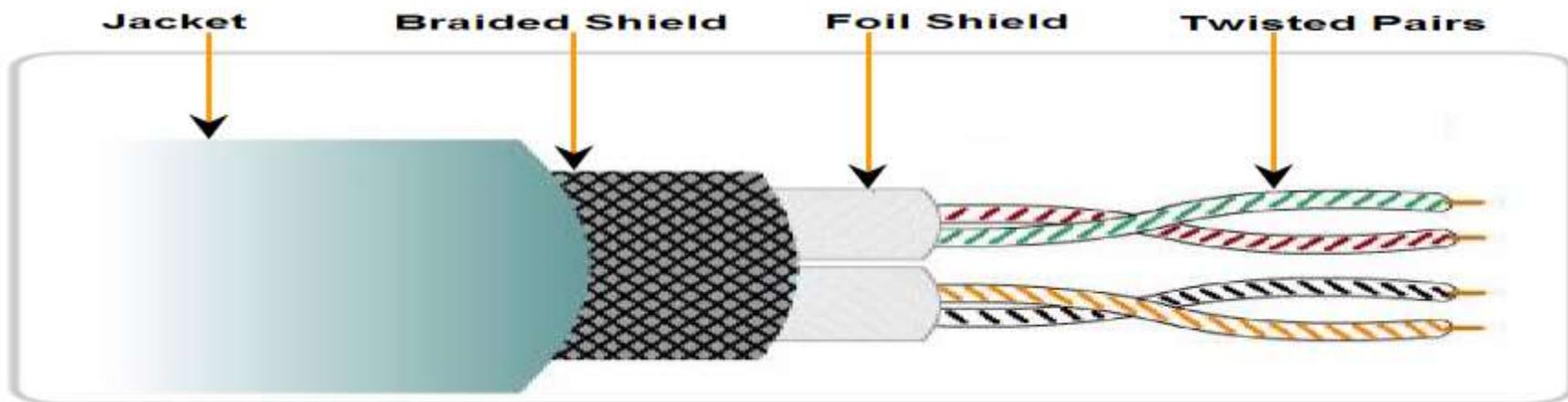
- **Copper Cable :** It can be run longer distances than Twisted pair Cables. Speed: 10-100Mbps Cost: Inexpensive Media and connector size: Medium Maximum cable length: 500m



Physical Layer

Shielded Twisted Pair :

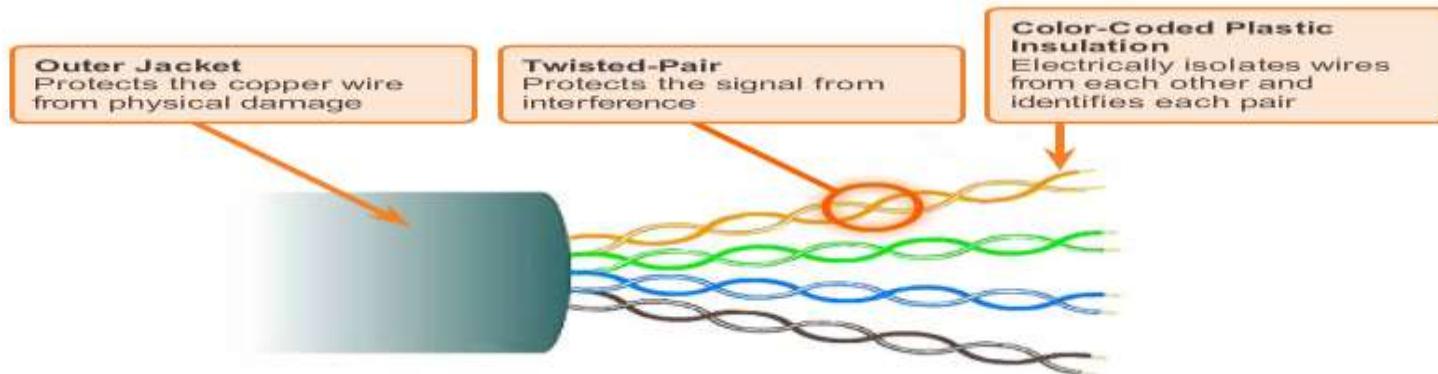
- Speed: 0-100Mbps
- Cost: Moderate
- Media and connector size: Medium to large
- Maximum cable length: 100m



Physical Layer

Unshielded Twisted Pair :

- UTP is a four-pair wire medium used in a variety of networks.
- Speed: 10-100-1000 Mbps*
- Cost: Least Expensive
- Media and connector size: Small
- Maximum cable length: 100m * (Depending on the quality/category of cable)

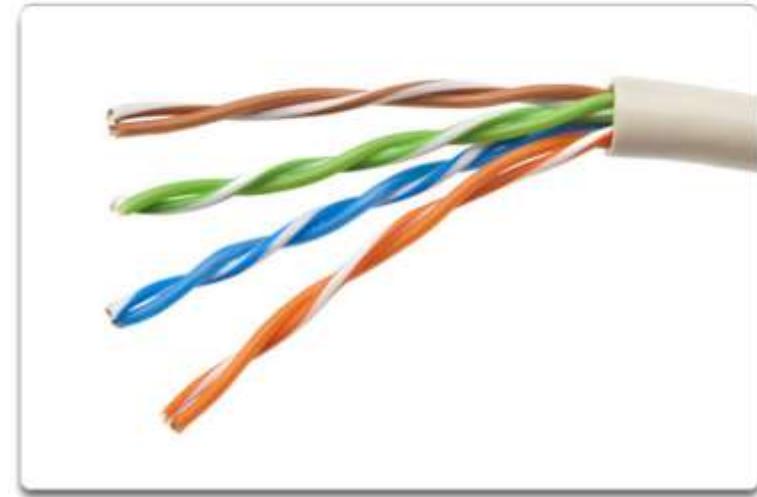


Physical Layer

Properties of Unshielded Twisted Pair :

UTP cable does not use shielding to counter the effects of EMI . Instead, cable designers have discovered that they can limit the negative effect of crosstalk by:

- Varying the number of twists per wire pair



Physical Layer

Unshielded Twisted Pair connectors :

RJ-45 UTP Plugs

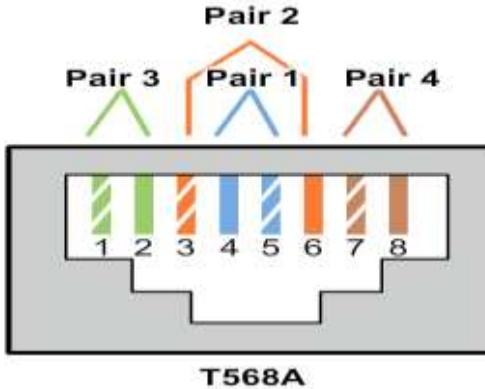


RJ-45 UTP Socket

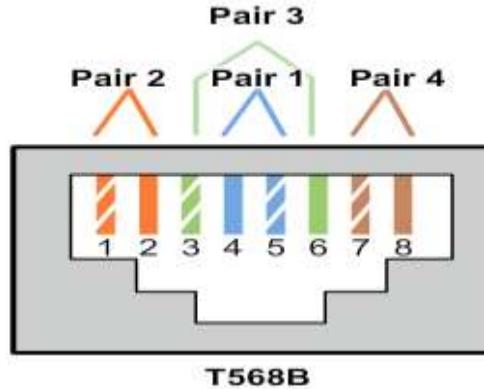


Physical Layer

Types of Unshielded Twisted Pair :



T568A



T568B

Cable Type	Standard	Application
Ethernet Straight-through	Both ends T568A or both ends T568B	Connects a network host to a network device such as a switch or hub.
Ethernet Crossover	One end T568A, other end T568B	<ul style="list-style-type: none">Connects two network hostsConnects two network intermediary devices (switch to switch, or router to router)
Rollover	Cisco proprietary	Connects a workstation serial port to a router console port, using an adapter.

Physical Layer

Testing Unshielded Twisted Pair cables :

After installation, a UTP cable tester should be used to test for the following parameters:

- Wire map
- Cable length
- Signal loss due to attenuation
- Crosstalk



Physical Layer

Fiber Optic Cabling :

After installation, a UTP cable tester should be used to test for the following parameters:

- Glass fiber carrying light pulses, each pulse a bit.
- Based on the Total Internal Reflection of Light.
- High-speed point-to-point transmission 10-100's Gbps

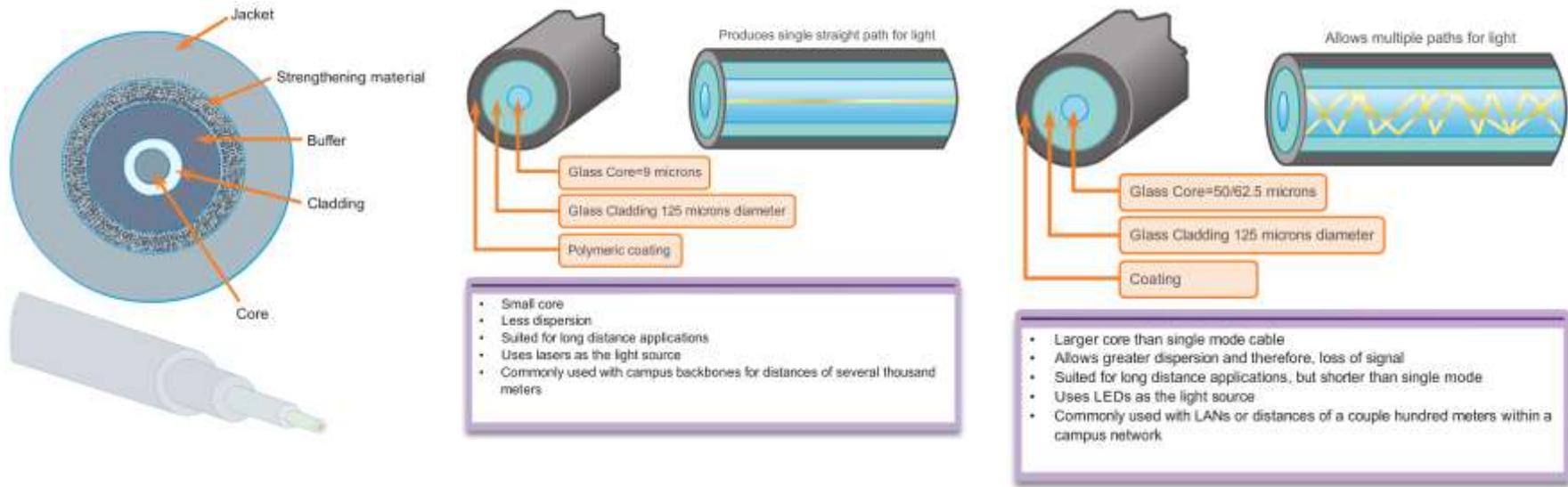
Fiber-optic cabling is now being used in four types of industry:

- Enterprise Networks
- Fiber-to-the-home (FTTH) and Access Networks
- Submarine Networks



Physical Layer

Fiber Media Cabling Design •

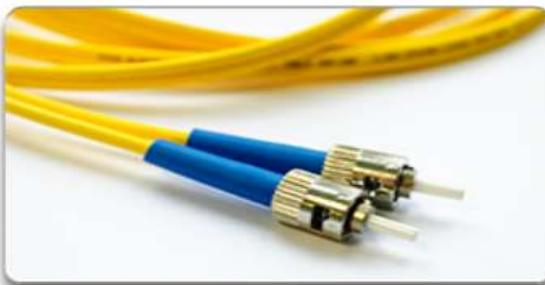


- **Single-mode fiber (SMF)** – uses only a single ray of light to carry data. Used for larger distances.
- **Multi-mode fiber (MMF)** – uses multiple rays of light to carry data. Less expensive than SMF.

Physical Layer

Fiber Connectors :

- ST (Straight-tip connector)
- SC (Subscriber connector)
- FC (Fiber Channel)
- LC (Lucent Connector)



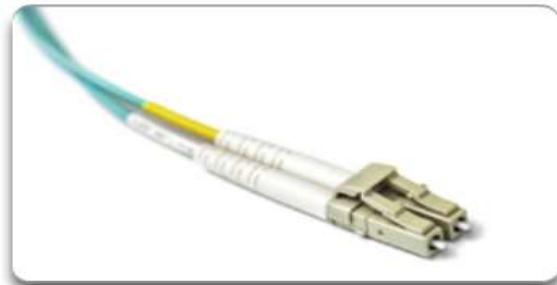
ST Connectors



SC Connectors



LC Connector



Duplex Multimode LC Connectors

Physical Layer

Fiber Versus Copper :

Implementation Issues	Copper Media	Fibre Optic
Bandwidth Supported	10 Mbps – 10 Gbps	10 Mbps – 100 Gbps
Distance	Relatively short (1 – 100 meters)	Relatively High (1 – 100,000 meters)
Immunity To EMI And RFI	Low	High (Completely immune)
Immunity To Electrical Hazards	Low	High (Completely immune)
Media And Connector Costs	Lowest	Highest
Installation Skills Required	Lowest	Highest
Safety Precautions	Lowest	Highest

Physical Layer

UnGuided Media

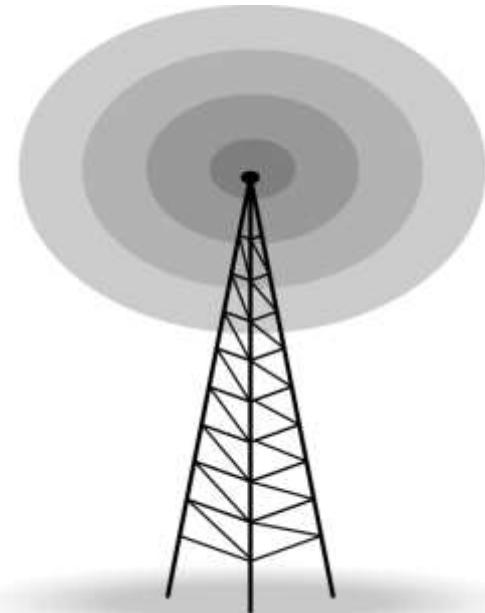
- An unguided transmission transmits the electromagnetic waves without using any physical medium. Therefore it is also known as **wireless transmission**.
- In unguided media, air is the media through which the electromagnetic energy can flow easily.

Physical Layer

UnGuided Media

Radio waves

- Radio waves are the electromagnetic waves that are transmitted in all the directions of free space.
- Radio waves are omnidirectional, i.e., the signals are propagated in all the directions.
- The range in frequencies of radio waves is from 3Khz to 1 khz.
- In the case of radio waves, the sending and receiving antenna are not aligned, i.e., the wave sent by the sending antenna can be received by any receiving antenna.
- An example of the radio wave is **FM radio**.



Omnidirectional antenna

Physical Layer

UnGuided Media

Applications Of Radio waves:

- A Radio wave is useful for multicasting when there is one sender and many receivers.
- An FM radio, television, cordless phones are examples of a radio wave.

Advantages Of Radio transmission:

- Radio transmission is mainly used for wide area networks and mobile cellular phones.
- Radio waves cover a large area, and they can penetrate the walls.
- Radio transmission provides a higher transmission rate.

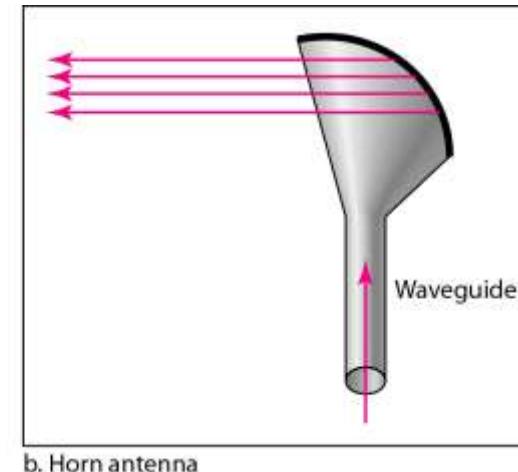
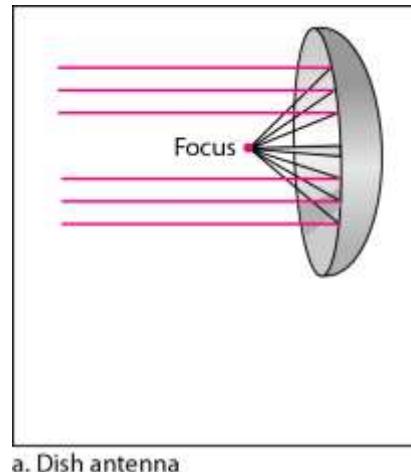
Physical Layer

UnGuided Media: Micro Waves

Micro Waves includes a line of sight transmission that is the sending and receiving antennas that need to be properly aligned with each other. The distance is directly proportional to the height of the antenna which is covered by the signal. In mobile phone communication and television distribution, these are majorly used.

Applications of Micro Waves

Due to the unidirectional properties of Micro Waves, they are very useful when unicast (one-to-one) communication is needed between the sender and the receiver. Cellular phones, satellite networks, and wireless LANs are using Micro Waves.



Physical Layer

UnGuided Media: Micro Waves

Two types of Microwave Transmission are as follows,

1. Terrestrial Microwave
2. Satellite Microwave

Microwave Transmission

Physical Layer

UnGuided Media: Micro Waves

1. Terrestrial Microwave

The frequency of Electromagnetic waves between 300 MHz and 300 GHz are called microwaves. These waves are unidirectional. Whenever through an antenna microwave are transmitting, they can be narrowly focused. That is the sending and receiving antennas need to be aligned.

Characteristics of microwaves

- It is inexpensive for short distance expensive as it requires a higher tower for a longer distance.
- Due to environmental conditions and antenna size attenuation (loss of signal) occurs.
- There is a capacity in very high-frequency microwaves that they cannot penetrate walls. This characteristic can be a disadvantage of microwaves if the receiver is inside the buildings.

Physical Layer

UnGuided Media: Micro Waves

Terrestrial Microwave

Advantages

- Microwave transmission is cheaper than using cables.
- It does not require any land for the installation of cables that is free from land acquisition.
- Microwave transmission provides easy communication.

Disadvantages

- Bandwidth is limited in microwave transmission.
- A signal can be moved out of phase and any environmental change such as rain, wind can distort the signal so these signals are susceptible to weather conditions.
- Cause of eavesdropping insecure communication occurs in which any user can catch the signal in the air by using its antenna.

Physical Layer

UnGuided Media: Micro Waves

2. Satellite Microwave

A satellite is an entity that revolves around the earth at a certain height. Satellite communication offers more flexibility than fiber optic and cable systems. We can transmit signals from any point on the globe by using satellite transmission.

How does a Satellite work?

The satellite receives the signal that is transmitted from the earth station, and it amplifies these signals. It is retransmitted the amplified signal to another earth station.

Satellite transmission is much like the line-of-sight transmission in which one of the stations is a satellite orbiting the earth. The principle is the same as the terrestrial microwave. Signals still travel in straight lines in satellite transmission.

Physical Layer

UnGuided Media: Micro Waves

2. Satellite Microwave

Features of Satellite Microwave

- It provides transmission capability to and from any location on earth.
- Deployment of Satellite microwaves for orbiting satellites is difficult.

Physical Layer

UnGuided Media: Micro Waves

2. Satellite Microwave

Advantages of Satellite Microwave

- High-quality communication available to undeveloped parts of the world without requiring a huge investment in the ground-based infrastructure.
- It is used in a variety of applications such as radio/TV signal broadcasting, weather forecasting, radio/TV signal broadcasting, mobile communication and mobile, and wireless communication applications.
- The coverage area of a terrestrial microwave is less than the satellite microwave.

Disadvantages of Satellite Microwave

- The manufacturing cost is very high of satellite and very expensive to launch a satellite.
- Transmission can go down in bad weather.

Physical Layer

UnGuided Media

Infrared

- An infrared transmission is a wireless technology used for communication over short ranges.
- The frequency of the infrared in the range from 300 GHz to 400 THz.
- It is used for short-range communication such as data transfer between two cell phones, TV remote operation, data transfer between a computer and cell phone resides in the same closed area.

Physical Layer

UnGuided Media

Characteristics Of Infrared:

- It supports high bandwidth, and hence the data rate will be very high.
- Infrared waves cannot penetrate the walls. Therefore, the infrared communication in one room cannot be interrupted by the nearby rooms.
- An infrared communication provides better security with minimum interference.
- Infrared communication is unreliable outside the building because the sun rays will interfere with the infrared waves.

Physical Layer

UnGuided Media

Characteristics Of Infrared:

- It supports high bandwidth, and hence the data rate will be very high.
- Infrared waves cannot penetrate the walls. Therefore, the infrared communication in one room cannot be interrupted by the nearby rooms.
- An infrared communication provides better security with minimum interference.
- Infrared communication is unreliable outside the building because the sun rays will interfere with the infrared waves.

