RGPVNOTES.IN

Program : **B.E**

Subject Name: **Advance Computer Networks**

Subject Code: **CS-8004**

Semester: **8th**

Advance Computer Networks
Subject Notes: UNIT-I

Computer Network

A **computer network** is a set of **computers** connected together for the purpose of sharing resources. The most common resource shared today is connection to the Internet. Other shared resources can include a printer or a file server.

#Goals

- Several machines can share printers, tape drives, etc.
- Reduced cost
- Resource and load sharing
- Programs do not need to run on a single machine
- High reliability
- If a machine goes down, another can take over
- Mail and communication

#Components

A data communications system has five components.

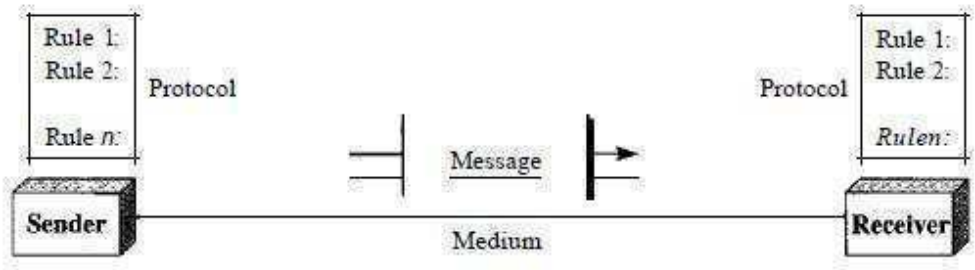

Fig. 1.1 Computer Network: Components

1. Message. The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.
2. Sender. The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.
3. Receiver. The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.
4. Transmission medium. The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves
5. Protocol. A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating.

#ISO-OSI Reference Model

#Principles of OSI Reference Model

The OSI reference model has 7 layers. The principles that were applied to arrive at the seven layers can be briefly summarized as follows:

1. A layer should be created where a different abstraction is needed.
2. Each layer should perform a well-defined function.
3. The function of each layer should be chosen with an eye toward defining internationally standardized protocols.

4. The layer boundaries should be chosen to minimize the information flow across the interfaces.
5. The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity and small enough that architecture does not become unwieldly.

Feature of OSI Model:

1. Big picture of communication over network is understandable through this OSI model.
2. We see how hardware and software work together.
3. We can understand new technologies as they are developed.
4. Troubleshooting is easier by separate networks.
5. Can be used to compare basic functional relationships on different networks.

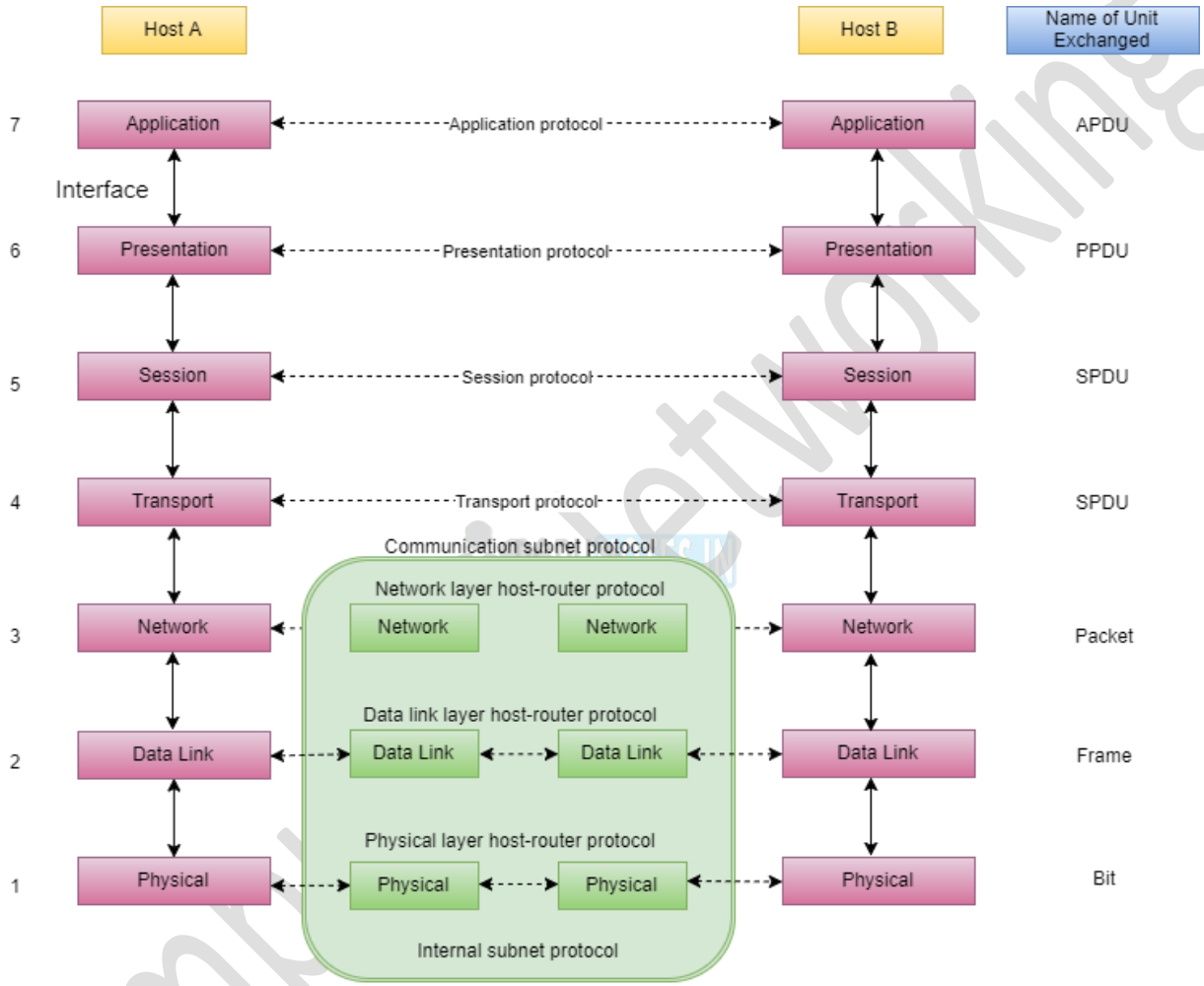

Fig. 1.2 OSI Reference Model

#Description of Different Layers:

Layer 1: The Physical Layer:

1. It is the lowest layer of the OSI Model.
2. It activates, maintains and deactivates the physical connection.
3. It is responsible for transmission and reception of the unstructured raw data over network.
4. Voltages and data rates needed for transmission is defined in the physical layer.
5. It converts the digital/ analog bits into electrical signal or optical signals.
6. Data encoding is also done in this layer.

The functions of the physical layer are:

1. **Bit synchronization**: The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level.

2. **Bit rate control**: The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
3. **Physical topologies**: Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star or mesh topology.
4. **Transmission mode**: Physical layer also defines the way in which the data flows between the two connected devices. The various transmission modes possible are: Simplex, half-duplex and full-duplex.

Layer 2: Data Link Layer:

1. Data link layer synchronizes the information which is to be transmitted over the physical layer.
2. The main function of this layer is to make sure data transfer is error free from one node to another, over the physical layer.
3. Transmitting and receiving data frames sequentially is managed by this layer.
4. This layer sends and expects acknowledgements for frames received and sent respectively. Resending of non-acknowledgement received frames is also handled by this layer.
5. This layer establishes a logical layer between two nodes and also manages the Frame traffic control over the network. It signals the transmitting node to stop, when the frame buffers are full.

The functions of the data Link layer are:

1. **Framing**: Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
2. **Physical addressing**: After creating frames, Data link layer adds physical addresses (MAC address) of sender and/or receiver in the header of each frame.
3. **Error control**: Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
4. **Flow Control**: The data rate must be constant on both sides else the data may get corrupted thus; flow control coordinates that amount of data that can be sent before receiving acknowledgement.
5. **Access control**: When a single communication channel is shared by multiple devices, MAC sub-layer of data link layer helps to determine which device has control over the channel at a given time.

Layer 3: The Network Layer:

1. It routes the signal through different channels from one node to other.
2. It acts as a network controller. It manages the Subnet traffic.
3. It decides by which route data should take.
4. It divides the outgoing messages into packets and assembles the incoming packets into messages for higher levels.

The functions of the Network layer are:

1. **Routing**: The network layer protocols determine which route is suitable from source to destination. This function of network layer is known as routing.
2. **Logical Addressing**: In order to identify each device on internetwork uniquely, network layer defines an addressing scheme. The sender & receiver's IP address are placed in the header by network layer. Such an address distinguishes each device uniquely and universally.

Layer 4: Transport Layer:

1. It decides if data transmission should be on parallel path or single path.
2. Functions such as Multiplexing, Segmenting or Splitting on the data are done by this layer
3. It receives messages from the Session layer above it, converts the message into smaller units and passes it on to the Network layer.
4. Transport layer can be very complex, depending upon the network requirements.

The functions of the transport layer are:

1. **Segmentation and Reassembly**: This layer accepts the message from the (session) layer , breaks the message into smaller units . Each of the segments produced has a header associated with it. The transport layer at the destination station reassembles the message.
2. **Service Point Addressing**: In order to deliver the message to correct process, transport layer header includes a type of address called service point address or port address. Thus by specifying this address, transport layer makes sure that the message is delivered to the correct process.

The services provided by transport layer:

1. **Connection Oriented Service**: It is a three-phase process which include
   – Connection Establishment
   – Data Transfer
   – Termination / disconnection
   In this type of transmission, the receiving device sends an acknowledgment, back to the source after a packet or group of packet is received. This type of transmission is reliable and secure.
2. **Connection less service**: It is a one phase process and includes Data Transfer. In this type of transmission, the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices. Connection oriented Service is more reliable than connection less Service.

Layer 5: The Session Layer:

1. Session layer manages and synchronize the conversation between two different applications.
2. Transfer of data from source to destination session layer streams of data are marked and are resynchronized properly, so that the ends of the messages are not cut prematurely, and data loss is avoided.

The functions of the session layer are:

1. **Session establishment, maintenance and termination:** The layer allows the two processes to establish, use and terminate a connection.
2. **Synchronization:** This layer allows a process to add checkpoints which are considered as synchronization points into the data. These synchronization point help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
3. **Dialog Controller:** The session layer determines which device will communicate first and the amount of data that will be sent.

Layer 6: The Presentation Layer:

1. Presentation layer takes care that the data is sent in such a way that the receiver will understand the information (data) and will be able to use the data.
2. While receiving the data, presentation layer transforms the data to be ready for the application layer.
3. Languages (syntax) can be different of the two communicating systems. Under this condition presentation layer plays a role of translator.
4. It performs Data compression, Data encryption, Data conversion etc.

The functions of the presentation layer are:

1. **Translation:** For example, ASCII to EBCDIC.
2. **Encryption/ Decryption:** Data encryption translates the data into another form or code. The encrypted data is known as the cipher text and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.
3. **Compression:** Reduces the number of bits that need to be transmitted on the network.

Layer 7: Application Layer:

1. It is the topmost layer.
2. Transferring of files disturbing the results to the user is also done in this layer. Mail services, directory services, network resource etc are services provided by application layer.
3. This layer mainly holds application programs to act upon the received and to be sent data.

The functions of the Application layer are:

1. Network Virtual Terminal
2. FTAM-File transfer access and management
3. Mail Services
4. Directory Services

Merits of OSI reference model:

1. OSI model distinguishes well between the services, interfaces and protocols.
2. Protocols of OSI model are very well hidden.
3. Protocols can be replaced by new protocols as technology changes.
4. Supports connection-oriented services as well as connectionless service.

Demerits of OSI reference model:

1. Model was devised before the invention of protocols.
2. Fitting of protocols is tedious task.
3. It is just used as a reference model.

#Comparison of the OSI and TCP/IP Reference Models:

OSI (Open System Interconnection)	TCP/IP (Transmission Control Protocol / Internet Protocol)
1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	1. TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
2. In OSI model the transport layer guarantees the delivery of packets.	2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
3. Follows vertical approach.	3. Follows horizontal approach.
4. OSI model has a separate Presentation layer and Session layer.	4. TCP/IP does not have a separate Presentation layer or Session layer.
5. Transport Layer is Connection Oriented.	5. Transport Layer is both Connection Oriented and Connection less.
6. Network Layer is both Connection Oriented and Connection less.	6. Network Layer is Connection less.
7. OSI is a reference model around which the networks are built. Generally, it is used as a guidance tool.	7. TCP/IP model is, in a way implementation of the OSI model.
8. Network layer of OSI model provides both connection oriented and connectionless service.	8. The Network layer in TCP/IP model provides connectionless service.
9. OSI model has a problem of fitting the protocols into the model.	9. TCP/IP model does not fit any protocol
10. Protocols are hidden in OSI model and are easily replaced as the technology changes.	10. In TCP/IP replacing protocol is not easy.

11. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	11. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
12. It has 7 layers	12. It has 4 layers

#Computer Network's: Classifications & Types.

There are three types of network classification

1) LAN (Local area network)
2) MAN (Metropolitan Area network)
3) WAN (Wide area network)

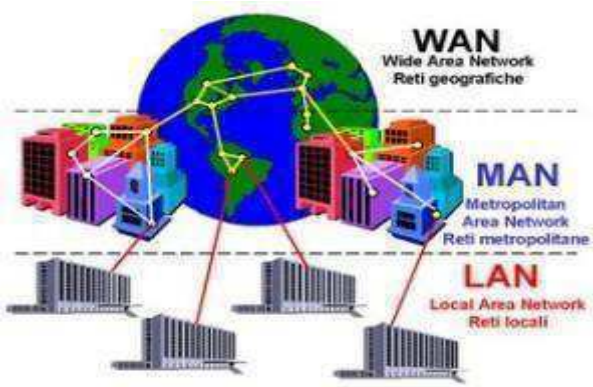

Fig. 1.5 Computer Network: Classifications

1) Local area network (LAN)

LAN is a group of the computers placed in the same room, same floor, or the same building so they are connected to each other to form a single network to share their resources such as disk drives, data, CPU, modem etc. LAN is limited to some geographical area less than 2 km. Most of LAN is used widely is an Ethernet system of the bus topology.

Characteristics of LAN

LAN connects the computer in a single building; block and they are working in any limited area less than 2 km.

Media access control methods in a LAN, the bus-based Ethernet and token ring.

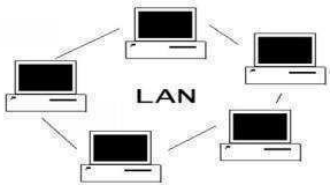

Fig. 1.6 Local area network

2) Metropolitan Area network (MAN)

The metropolitan area network is a large computer network that expands a Metropolitan area or campus. Its geographic area between a WAN and LAN. Its expand round 50km devices used are modem and wire/cable.

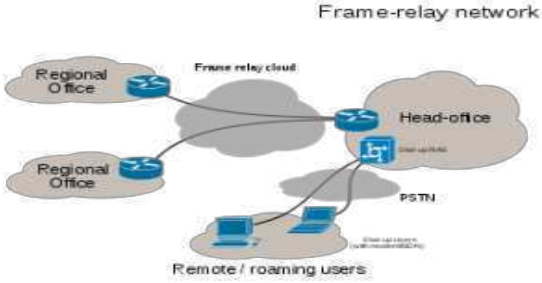

Fig. 1.7 Metropolitan Area network

Characteristics of MAN

1) Its covers the towns and cities (50km)
2) MAN is used by the communication medium for optical fibre cables, it also used for other media.

3) Wide area Network (WAN)

The wide area network is a network which connects the countries, cities or the continents, it is a public communications links. The most popular example of a WAN is the internet. WAN is used to connect LAN so the users and the computer in the one location can communicate with each other.

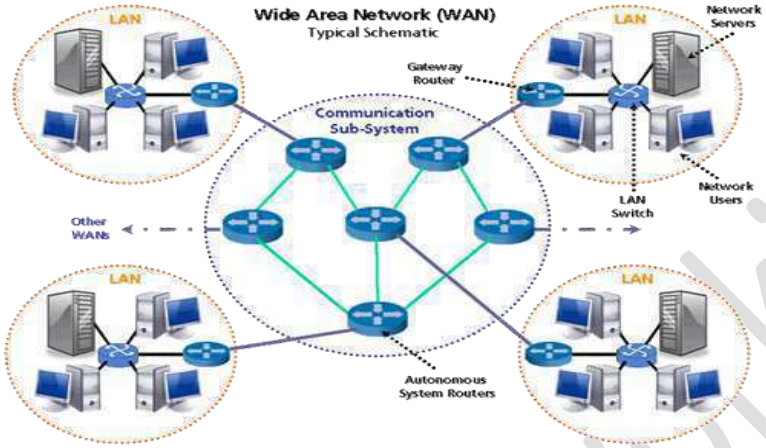

Fig. 1.8 Wide area Network

Characteristics of WAN

1) Its covers the large distances (More than 100 KM).
2) Communication medium used are satellite, telephones which are connected by the routers.

 # Communication Media:

Communication medium refers to the physical channel through which data is sent and received. Data is sent in the form of voltage levels which make up the digital signal. A digital signal consists of 0s and 1s; essentially, a 1 corresponds to a high voltage, while a 0 corresponds to a low voltage.

The speed of data transmission or data rate depends upon the type of medium being used in the network. There are basically two types of networks:

- Wired network
- Wireless network

Wired Network

In a wired network, data is transmitted over a physical medium. There are three types of physical cables used in a wired network. Transmission medium is the means through which we send our data from one place to another. The first layer (physical layer) of Communication Networks OSI Seven layer model is dedicated to the transmission media.

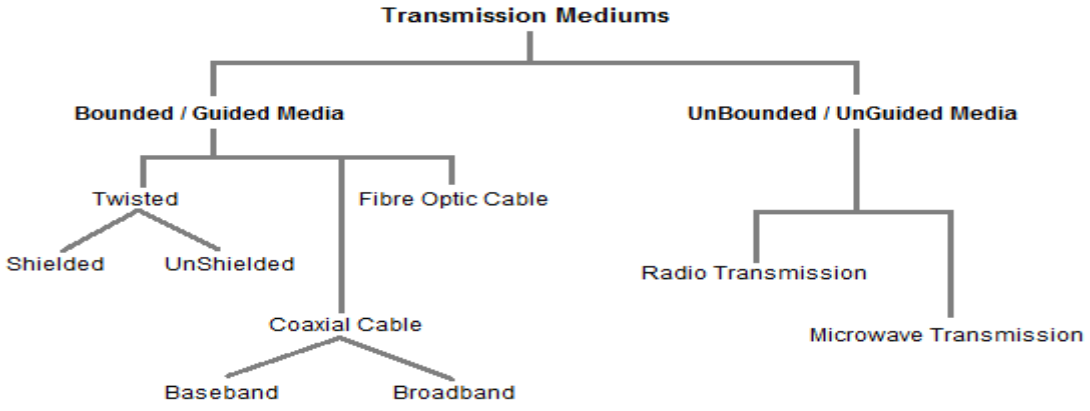

Fig. 1.9 Transmission Medium

Factors to be considered while choosing Communication Media:

1. Transmission Rate
2. Cost and Ease of Installation
3. Resistance to Environmental Conditions
4. Distances
5. Bounded/Guided Transmission Media

It is the transmission media in which signals are confined to a specific path using wire or cable. The types of **Bounded/ Guided** are discussed below.

- **Twisted Pair Cable**

This cable is the most commonly used and is cheaper than others. It is lightweight, cheap, can be installed easily, and they support many different types of network. Some important points :

- Its frequency range is 0 to 3.5 kHz.
- Typical attenuation is 0.2 dB/Km @ 1kHz.
- Typical delay is 50 μs/km.
- Repeater spacing is 2km.
- Twisted Pair is of two types :
- Unshielded Twisted Pair (UTP)
- Shielded Twisted Pair (STP)

- **Unshielded Twisted Pair Cable**

It is the most common type of telecommunication when compared with Shielded Twisted Pair Cable which consists of two conductors usually copper, each with its own colour plastic insulator. Identification is the reason behind colored plastic insulation.

UTP cables consist of 2 or 4 pairs of twisted cable. Cable with 2 pair use RJ-11 connector and 4 pair cable use RJ-45 connector.

Advantages:

1. Installation is easy
2. Flexible
3. Cheap
4. It has high speed capacity,
5. 100 meter limit
6. Higher grades of UTP are used in LAN technologies like Ethernet.
7. It consists of two insulating copper wires (1mm thick). The wires are twisted together in a helical form to reduce electrical interference from similar pair.

Disadvantages:

1. Bandwidth is low when compared with Coaxial Cable
2. Provides less protection from interference.
3. Shielded Twisted Pair Cable
4. This cable has a metal foil or braided-mesh covering which encases each pair of insulated conductors. Electromagnetic noise penetration is prevented by metal casing. Shielding also eliminates crosstalk.

It has same attenuation as unshielded twisted pair. It is faster the unshielded and coaxial cable. It is more expensive than coaxial and unshielded twisted pair.

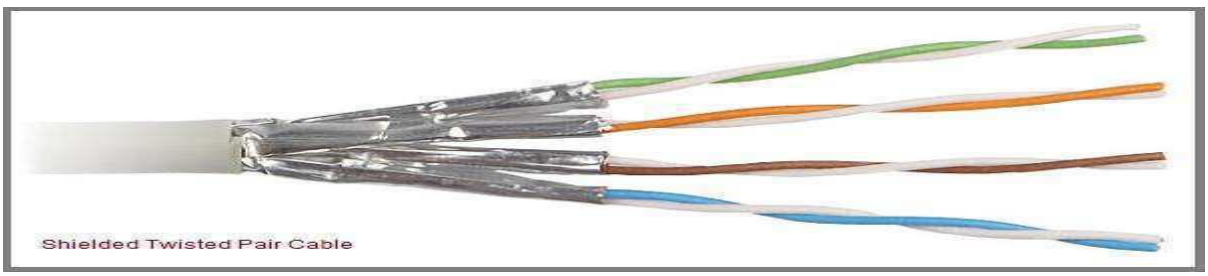

Fig. 1.10 Shielded Twisted Pair Cable

Advantages:

1. Easy to install
2. Performance is adequate
3. Can be used for Analog or Digital transmission
4. Increases the signalling rate
5. Higher capacity than unshielded twisted pair
6. Eliminates crosstalk

Disadvantages:

1. Difficult to manufacture
2. Heavy

- **Coaxial Cable**

Coaxial is called by this name because it contains two conductors that are parallel to each other. Copper is used in this as centre conductor which can be a solid wire or a standard one. It is surrounded by PVC installation, a sheath which is encased in an outer conductor of metal foil, barid or both.
Outer metallic wrapping is used as a shield against noise and as the second conductor which completes the circuit. The outer conductor is also encased in an insulating sheath. The outermost part is the plastic cover which protects the whole cable.

1. Here the most common coaxial standards.
2. 50-Ohm RG-7 or RG-11 : used with thick Ethernet.
3. 50-Ohm RG-58 : used with thin Ethernet
4. 75-Ohm RG-59 : used with cable television
5. 93-Ohm RG-62 : used with ARCNET.

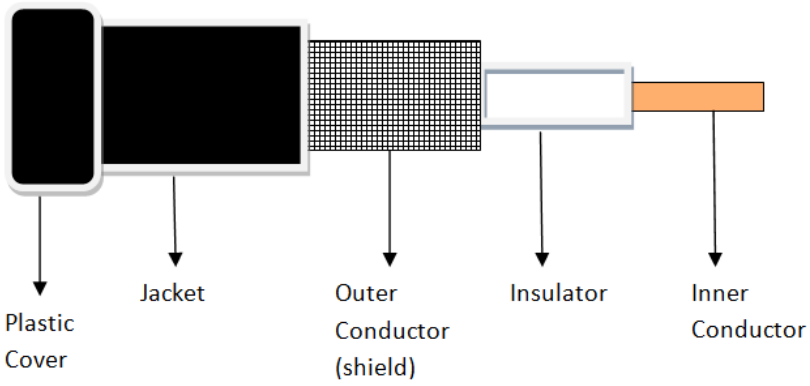

Fig. 1.11 Coxial Cable

There are two types of Coaxial cables:

Baseband

This is a 50 ohm (Ω) coaxial cable which is used for digital transmission. It is mostly used for LAN's. Baseband transmits a single signal at a time with very high speed. The major drawback is that it needs amplification after every 1000 feet.

Broadband

This uses analog transmission on standard cable television cabling. It transmits several simultaneous signal using different frequencies. It covers large area when compared with Baseband Coaxial Cable.

Advantages:

1. Bandwidth is high
2. Used in long distance telephone lines.
3. Transmits digital signals at a very high rate of 10Mbps.
4. Much higher noise immunity
5. Data transmission without distortion.
6. The can span to longer distance at higher speeds as they have better shielding when compared to twisted pair cable.

Disadvantages:

1. Single cable failure can fail the entire network.
2. Difficult to install and expensive when compared with twisted pair.
3. If the shield is imperfect, it can lead to grounded loop.

- **Optical Fiber**

An optical fiber or optical fibre is a flexible, transparent fiber made by drawing glass (silica) or plastic to a diameter slightly thicker than that of a human hair. Optical fibers are used most often as a means to transmit light between the two ends of the fiber and find wide usage in fiber-optic communications, where they permit transmission over longer distances and at higher bandwidths (data rates) than wire cables. Fibers are used instead of metal wires because signals travel along them with less loss; in addition, fibers are immune to electromagnetic interference, a problem from which metal wires suffer excessively. Fibers are also used for illumination, and are wrapped in bundles so that they may be used to carry images, thus allowing viewing in confined spaces, as in the case of a fiberscope. Specially designed fibers are also used for a variety of other applications, some of them being fiber optic sensors and fiber lasers.
These are similar to coaxial cable. It uses electric signals to transmit data. At the centre is the glass core through which light propagates.
In multimode fibers, the core is 50microns, and in single mode fibers, the thickness is 8 to 10 microns.
The core in fiber optic cable is surrounded by glass cladding with lower index of refraction as compared to core to keep all the light in core. This is covered with a thin plastic jacket to protect the cladding. The fibers are grouped together in bundles protected by an outer shield.
Fiber optic cable has bandwidth more than 2 gbps (Gigabytes per Second)

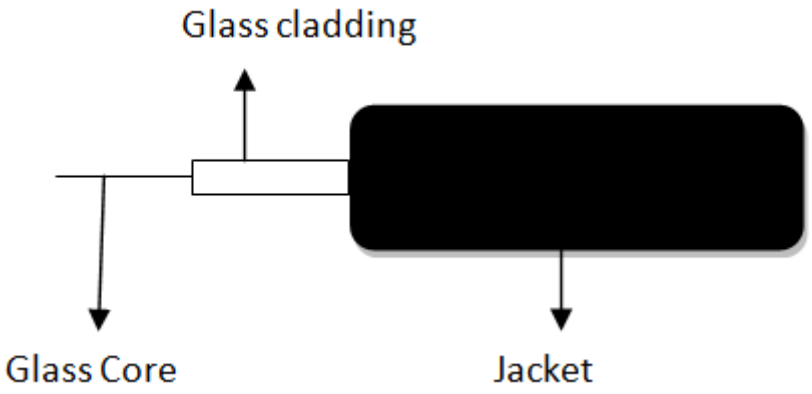

Fig. 1.12 Optical Fiber

Advantages:

1. Provides high quality transmission of signals at very high speed.
2. These are not affected by electromagnetic interference, so noise and distortion is very less.
3. Used for both analog and digital signals.

Disadvantages:

1. It is expensive
2. Difficult to install.
3. Maintenance is expensive and difficult.
4. Do not allow complete routing of light signals.

It is the transmission media in which signals are confined to a specific path using wire or cable. The types of **Unbounded/ Unguided** are discussed below.

- **Physics and Velocity of Propagation of Light**

Whereas the velocity of some particle is a quantity which is based on a fairly simple and unambiguous concept, the velocity of light (as of other wave phenomena) is a much more sophisticated matter. There

are different kinds of velocities, which are different conceptually and can (particularly for light propagation in media) have substantially different values:

1. The phase velocity is the velocity with which phase fronts propagate.
2. The group velocity determines the speed with which intensity maxima propagate (e.g. the peaks of pulses).
3. The velocity of information transport can differ from both phase and group velocity.

- **Electromagnetic waves**

EM waves are energy transported through space in the form of periodic disturbances of electric and magnetic fields.
EM waves travel through space at the same speed, c = 2.99792458 x 108 m/s, commonly known as the speed of light.
An EM wave is characterized by a frequency and a wavelength.
These two quantities are related to the speed of light by the equation speed of light = frequency x wavelength
The frequency (or wavelength) of an EM wave depends on its source. There is a wide range of frequency encountered in our physical world, ranging from the low frequency of the electric waves generated by the power transmission lines to the very high frequency of the gamma rays originating from the atomic nuclei. This wide frequency range of electromagnetic waves constitute the Electromagnetic Spectrum

#Network Standardization

International Organization for Standardization One of the most important standards-making bodies is the International Organization for Standardization (ISO), 2 which makes technical recommendations about data communication interfaces .ISO is based in Geneva, Switzerland. The membership is composed of the national standards organizations of each ISO member country.

International Telecommunications Union—Telecommunications Group the Telecommunications Group (ITU-T) is the technical standards-setting organization of the United Nations International Telecommunications Union, which is also based in Geneva. ITU is composed of representatives from about 200-member countries. Membership was originally focused on just the public telephone companies in each country, but a major reorganization in 1993 changed this, and ITU now seeks members among public- and private-sector organizations who operate computer or communications networks (e.g., RBOCs) or build software and equipment for them (e.g., AT&T).

American National Standards Institute: The American National Standards Institute (ANSI) is the coordinating organization for the U.S. national system of standards for both technology and nontechnology ANSI has about 1,000 members from both public and private organizations in the United States. ANSI is a standardization organization, not a standards-making body, in that it accepts standards developed by other organizations and publishes them as American standards. Its role is to coordinate the development of voluntary national standards and to interact with ISO to develop national standards that comply with ISO's international recommendations. ANSI is a voting participant in the ISO.

 # IEEE Standards

IEEE Standards Association (IEEE-SA) provides a, global, open, and collaborative platform for wireless communities that engage in, and enable the development of new, innovative, and relevant use cases and standards which, in turn, accelerate the time to market of consensus-developed technologies.

Specific areas of focus include:

- Mobile broadband network evolution
- Technology interoperability

- Enabling IoT and Smart Cities (including public safety)

Inclusive to this is the ability to support addressing the following technological considerations:

- Integration of networking, computing, and storage resources into one programmable and unified infrastructure. This includes design principles such as resources, connectivity, and service enablers.
- Multi-tenancy models
- Sustainability, scalability, security, and privacy management
- Spectrum
- Software enablement for SDN, NFV, Mobile Edge, Fog Computing, Virtualization, etc.

IEEE-SA adds value in this emerging space by:

1. Supporting the development of market driven constructs (SIG, Alliances, etc.,) while representing the interests of ourselves and our stakeholders (Societies, Councils, and Working Groups).
2. Addressing region-specific use cases, to ensure regional viability of standards and applications.
3. Offering add-on services, products, registries, and lifecycle elements and supporting the development of initiatives and APIs where applicable.

- **IEEE 802.2 Logical Link Control**

1. The technical definition for 802.2 is "the standard for the upper Data Link Layer sub layer also known as the Logical Link Control layer.
2. It is used with the 802.3, 802.4, and 802.5 standards (lower DL sub layers).
3. "802.2 "specify the general interface between the network layer (IP, IPX, etc) and the data link layer (Ethernet, Token Ring, etc).
4. IEEE 802.2 As the "translator" for the Data Link Layer.
5. 802.2 are concerned with managing traffic over the physical network.
6. It is responsible for flow and error control.
7. The Data Link Layer wants to send some data over the network, 802.2 Logical Link Control helps make this possible.
8. It also helps by identifying the line protocol, like NetBIOS, or Netware.
9. The LLC acts like a software bus allowing multiple higher layer protocols to access one or lower layer networks.
   For example, if you have a server with multiple network interface cards, the LLC will forward packers from those upper layer protocols to the appropriate network interface. This allows the upper layer protocols to not need specific knowledge of the lower layer networks in use.

- **IEEE 802.3 Ethernet**

1. 802.3 is the standard which Ethernet operates by.
2. It is the standard for CSMA/CD (Carrier Sense Multiple Access with Collision Detection).
3. This standard encompasses both the MAC and Physical Layer standards. CSMA/CD is what Ethernet uses to control access to the network medium (network cable).
4. If there is no data, any node may attempt to transmit, if the nodes detect a collision, both stop transmitting and wait a random amount of time before retransmitting the data.
5. The original 802.3 standard is 10 Mbps (Megabits per second).
6. 802.3u defined the 100 Mbps (Fast Ethernet) standard, 802.3z/802.3ab defined 1000 Mbps Gigabit Ethernet, and 802.3ae define 10 Gigabit Ethernet.
7. Commonly, Ethernet networks transmit data in packets, or small bits of information.
8. A packet can be a minimum size of 72 bytes or a maximum of 1518 bytes. The most common topology for Ethernet is the star topology.

- **IEEE 802.5 Token Ring**
  1. Token Ring was developed primarily by IBM.
  2. Token ring is designed to use the ring topology and utilizes a token to control the transmission of data on the network.
  3. The token is a special frame which is designed to travel from node to node around the ring.
  4. When it does not have any data attached to it, a node on the network can modify the frame, attach its data and transmit.
  5. Each node on the network checks the token as it passes to see if the data is intended for that node, if it is; it accepts the data and transmits a new token.
  6. If it is not intended for that node, it retransmits the token on to the next node.
  7. The token ring network is designed in such a way that each node on the network is guaranteed access to the token at some point. This equalizes the data transfer on the network.
  8. This is different from an Ethernet network where each workstation has equal access to grab the available bandwidth, with the possible of a node using more bandwidth than other nodes.
  9. Token ring operated at a speed of about 4 Mbps and 16 Mbps. 802.5t allows for 100 Mbps speeds and 802.5v provides for 1 Gbps over fibber.
  10. Token ring can be run over a star topology as well as the ring topology.
  11. There are three major cable types for token ring: Unshielded twisted pair (UTP), Shielded twisted pair (STP), and fibber.
  12. Token ring utilizes a Multi-station Access Unit (MAU) as a central wiring hub. This is also sometimes called a MSAU when referring to token ring networks.

- **IEEE 802.11 Wireless Network Standards**
  1. 802.11 is the collection of standards setup for wireless networking.
  2. We are Familiar with 802.11a, 802.11b, 802.11g and latest one is 802.11n.
  3. Each standard uses a frequency to connect to the network and has a defined upper limit for data transfer speeds.802.11a been one of the first wireless standards.
     a) 802.11a operates in the 5 GHz radio band and can achieve a maximum of 54Mbps. wasn't as popular as the 802.11b standard due to higher prices and lower range.
     b) 802.11b operates in the 2.4 GHz band and supports up to 11 Mbps. Range of up to several hundred feet in theory. The first real consumer option for wireless and very popular.
     c) 802.11g is a standard in the 2.4 GHz band operating at 54Mbps.
  4. Since it operates in the same band as 802.11b, 802.11g is compatible with 802.11b equipment. 802.11a is not directly compatible with 802.11b or 802.11g since it operates in a different band. Wireless LANs primarily use CSMA/CA - Carrier Sense Multiple Access/Collision Avoidance.
  5. It has a "listen before talk" method of minimizing collisions on the wireless network. This results in less need for retransmitting data. Wireless standards operate within a wireless topology.

RGPVNOTES.IN

We hope you find these notes useful.

You can get previous year question papers at https://qp.rgpvnotes.in .

If you have any queries or you want to submit your study notes please write us at rgpvnotes.in@gmail.com

LIKE & FOLLOW US ON FACEBOOK
facebook.com/rgpvnotes.in