ଓଡ଼ିଶା ରାଜ୍ୟ ମୁକ୍ତ ବିଶ୍ୱବିଦ୍ୟାଳୟ, ସମ୍ବଲପୁର, ଓଡ଼ିଶା
Odisha State Open University, Sambalpur, Odisha
Established by an Act of Government of Odisha.

DIPLOMA IN CYBER SECURITY

DCS-02

Block

1

Data Communication and Networking

INTRODUCTION TO DATA COMMUNICATION AND NETWORKING

Unit – 1

Basic Concepts of Data Communication and Networking

Unit – 2

Network Reference Models

Unit – 3

Transmission Media and Network Devices

EXPERT COMMITTEE

Dr. P.K.Behera –Reader in Computer Science, Utkal University-**Member**
Dr. J.R Mohanty-Prof. & HOD Computer Science, KIIT University-**Member**
Dr.R.N.Behera-Senior Technical Director, NIC,Bhubaneswar-**Member**
Sh.Pabitrananda Patnaik-Scientist-E,NIC,Bhubaneswar-**Member**
Sh.Malaya Kumar Dash- Scientist-E,NIC,Bhubaneswar-**Member**
Dr.Bhagirathi Nayak-Professor and Head (IT & System)Sri Sri University-**Member**
Dr. Manoranjan Pradhan- Professor and Head CSE,GITA,Bhubaneswar-**Member**
Sh.V.S.Sandilya-Academic Consultant, Odisha State Open University-**Convener**

DIPLOMA IN CYBER SECURITY

Course Writer:
Chandrakant Mallick
Consultant (Academic)
School of Computer and Information Science
Odisha State Open University

Unit – 1
Basic Concepts of Data Communication and Networking

Structure

1.0 Introduction

Data communication technology deals with the means and methods of data transfer from one location to another. The developments of computing and communication technology lead to the evolution of computer networks.

Computer network is an interconnection of computers that are geographically distributed, but connected in such a manner to enable exchange of information among them. The main objective of data communication and computer network is sharing of resources (hardware and software) between any two devices or person in the world.

It this unit we will introduce the concepts of data communication and computer networks.

1.1 Objectives

After completion of the unit, you should be able to:

- Understand the meaning and conceptof data communication
- Know the characteristics and components of data communication system.
- Know different forms of data and their representation
- Identifyand differentiate data communication modes
- List the topologies used in setting networks.
- Compare the pros and cons of different topologies.
- Analyze various topologies and apply it in the application
- Define a computer network, identify the categories of computer networks and differentiate their characteristics.
- Understand the concepts of protocols and standards.
- Know different standard organizations in communications.

1.2 Data and Information

Data refers to a collection of raw facts and figures that can be stored and transmitted. Data can become **information** after being processed. Information enables us to take decisions. In the context of data communication we refer data that is transmitted in the form of message. The message can be in the form of text, images, audio, video etc. These data are encoded in to electromagnetic signals for transmission over a physical medium.

1.3 Data Communication

Data communication is the transfer of data or information from a source to a destination. The sender at the source transmits the data and the receiver receives the data at the destination.Thetransfer ofdata in the form of message is done between two devices over a transmission medium is known as a data communication system which also involves some hardware and software. The hardware part involves the sender and receiver devices and the intermediate devices through which the message is transmitted.The software part involves certain rules that guide data communication is called as a protocol. The following section describes the fundamental characteristics of a data communication process and is followed by the components that make up a data communications system.

1.3.1 Characteristics of Data Communication

The effectiveness of any data communications system depends upon the following four fundamental characteristics:

Delivery: The data should be delivered to the correctdestination and correct user.

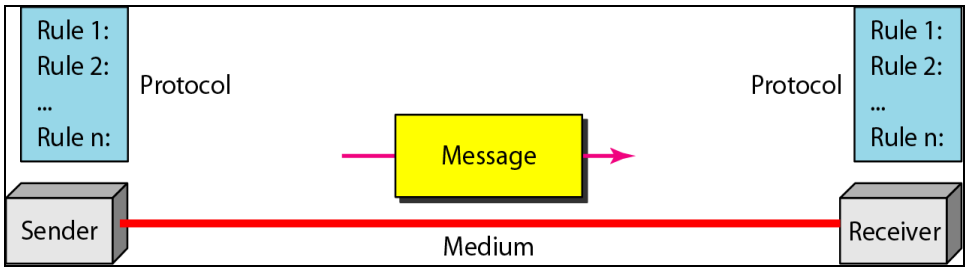
Accuracy: The communication system should deliver the dataaccurately, without introducing any errors. The data may get corrupted during transmission affecting the accuracy of the delivered data.

Timeliness: Audio and Video data has to be delivered in atimely manner without any delay; such a data delivery is called real time transmission of data.

Jitter: It is the variation in the packet arrival time. Uneven Jittermay affect the timeliness of data being transmitted.

1.3.2Components of Data CommunicationSystem

A Data Communication system has five components as shown in the diagram below:



Components of a Data Communication System

1. **Message**
   Message is the information to be communicated by the sender to the receiver.
2. **Sender**
   The sender is any device that is capable of sending the data (message).
3. **Receiver**
   The receiver is a device that the sender wants to communicate the data (message).
4. **Transmission Medium:**
   It is the path by which the message travels from sender to receiver.
5. **Protocol**
   A protocol is a set of rules that governs data communication. It is an agreed upon set or rules used by the sender and receiver to communicate data.

1.4 Data Representation

Data is collection of raw facts which is processed to produce information. There may be different forms in which data may be represented.

1.4.1 Types of data

Some of the forms of data that are used in data communication are as follows:

Text

Text includes combination of alphabets in small case as well as upper case.It is stored as a pattern of bits. Prevalent encoding system: ASCII, Unicode

Numbers

Numbers include combination of digits from 0 to 9.It is stored as a pattern of bits. Prevalent encoding system: ASCII, Unicode.

Images

An image is worth a thousand words. In computers images are digitally stored. A Pixel is the smallest element of an image. To put it in simple terms, a picture or image is a matrix of pixel elements.

Audio

Data can also be in the form of audio which can be recorded and broadcasted. Example: What we hear on the radio is a source of data or information. Audio data is continuous, not discrete.

Video

Video refers to broadcasting of data in form of moving picture along with audio.

1.4.2 Analog and Digital data

Data to be transmitted, data must be transformed in to electromagnetic signals. Electromagnetic signals can be either analog or digital. Accordingly data can be classified as analog and digital data.

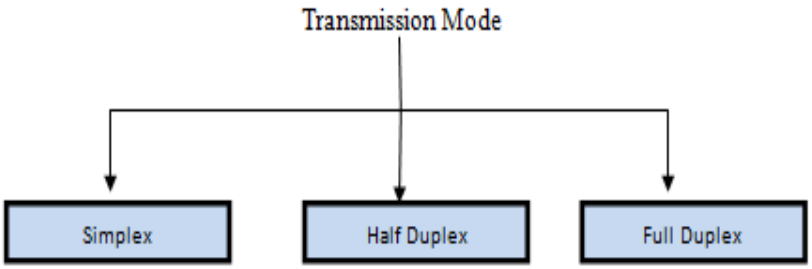
Analog datarefersto information that is represented in continuouswave forms. For example sound produced by human voice. When a person sings a song an analog wave is created in air. If that voice is captured by a microphone and converted in to analog signal and transmitted through analog medium or modulated to a digital signal.

Digital data refers to data that has discrete states. Digital data take on discrete set of values.

For example data stored in a computer in the form of 0s and 1s that can be converted in to digital signal or modulated in to an analog signal for transmission across a medium.

1.5 Data Transmission Modes

Two devices are said to be communicating with each other if they are able to send and receive data. Each device can act as a sender as well as a receiver. The data flow between the two devices can be in simplex, half duplex and full duplex modes.



Data Transmission Modes

1. Simplex

In Simplex, communication is unidirectional. Only one of the devices sends the data and the other one only receives the data. Example: A CPU sends data while a monitor only receives data.

2. Half Duplex

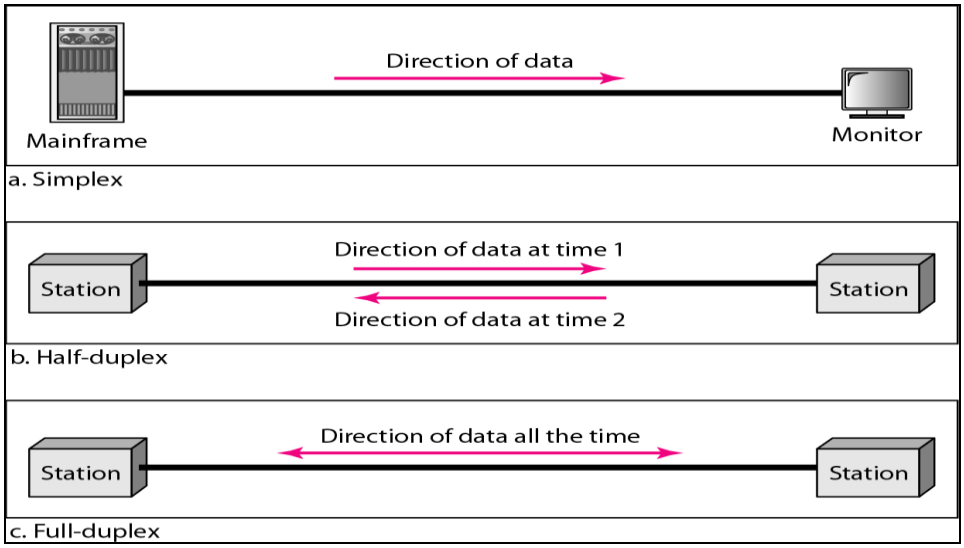
In half duplex both the stations can transmit as well as receive but not at the same time.

When one device is sending other can only receive and vice-versa (as shown in figure above.)

Example: A walkie-talkie.

3. Full Duplex

In Full duplex mode, both stations can transmit and receive at the same time.
Example: mobile phones.



Data Transmission Modes

1.6 Computer Networks

A Computer network is an interconnected collection of autonomous computers and other devices that use a common network language to share resources send data to and receive data from each other over a network media.

The computers are said to be interconnected if they are able to exchange information.

Each computer in the network is regarded as nodes. A node can also be any device capable of transmitting or receiving data. The communicating nodes have to be connected by communication links.

A computer network is a setup 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.

1.6.1 Need of Computer Networks

The important motivations for a computer network include the following.

a) Sharing of resources such as printers and expensive software and databases.
b) Serves as communication media for long distance communication
c) Provides high reliability and availability of data and information among the users of the network.
d) Provides economyof data storage and communication
e) Scalable to accommodate increasing number of users

f) Offers centralized administration
g) Connects people, buildings and organizations

1.6.2 Components of a network

Following are some of the major components of a computer network.

(i) Computers or work stations
(ii) Servers such as File Servers, Print Servers, Database Servers etc.
(iii) Printers, Faxes
(iv) Interconnecting devices such as switches, hubs, routers, bridges, gateways etc.
(v) Connectors, cables(coaxial, twisted pair or fiber optic)
(vi) A Network Interface Card (NIC) in each computer
(vii) Network Operating Systems

Advantages of Computer Networks

Following are some of the advantages of a computer network

a) **Increased Speed**: Network provides a fastest medium of data communication
b) **Reduced Cost**: It reduces the storage and maintenance and data transfer cost per unit.
c) **Improved Security**: It is now possible to protect the programs and files from illegal access.
d) **Centralized Administration**: A centralized server can store the important software's and provide controlled access to many users.
e) **Flexible Access**: It is possible for the authorized user to access their files from any computer connected in the network.

Disadvantages of Computer Networks

Major disadvantages of a computer network are as follows:

a) **High cost of installation:** The initial cost of installation of a computer network is high.
b) **Maintenance cost:** It requires proper and careful administration and maintenance by specialized technical person.
c) **Failure of Server:** If the file server goes down then the entire network comes to stand still.
d) **Cable fault:** The computers in the network are connected with the help of cables. If the backbone cable fails it causes the entire network failure.

1.6.3 Network Criteria

The most important criteria for a network to be efficient are performance reliability and security.

Performance

Performance of a network can be measured in many ways including transit time and response time.

Transit time is the amount of time required to transmit a message from one device to the other.

Response time is the time elapsed between a request and response.

Performance of a network can be ensured by achieving higher throughput and smaller delay times.Performance of a networkalso depends on other factors including the following.

(i) Number of users
(ii) Type of transmission medium
(iii)Network hardware and software.

Reliability

Reliability of a network depends on accuracy, frequency of failure, the time it takes to recover from failure and robustness in a catastrophe.

A computer network is said to be reliable if it provide higher level of accuracy, less frequency of failure, less recovery time and robust to catastrophic failure.

Security

Network Securityissues include protecting data from unauthorized access, virus and different types of attacks to access network resources.The network protocols provide security mechanisms to ensure protection of data from unauthorized access. A good network is protected from virus by specifically designed hardware and software.

1.7 Network Topology

The term topology, or more specifically, network topology, refers to the arrangement or physical layout of computers, cables, and other components on the network.

A network is consisting of two or more devices connected to each other through connecting links. The devices in the network can be connected in two ways.

(i) Point-to-point connection
(ii) Multi-point connection

(i) Point-to-point connection

A point-to-point connection provides a dedicated link between two devices. The entire capability of the link is reserved for transmission between these two devices.

(iii)Multi-point connection

Multipoint connection more than two devices share a single link. The capability of the link is shared among all users.

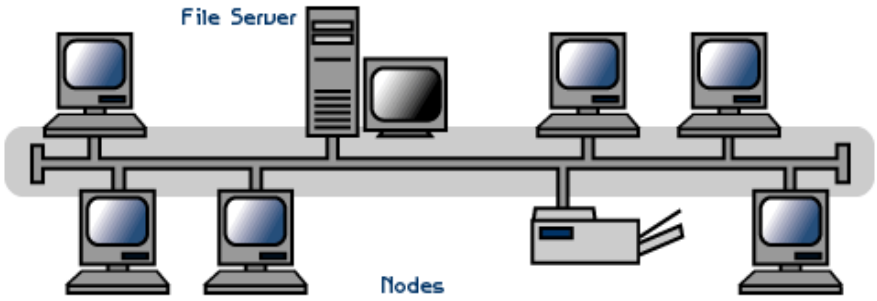
1.7.1 Types of topology

The topology of a network is the geometric representation of the relationship of all the links connecting the devices (nodes). Usually network topologies are of following type.

1. Bus topology
2. Star topology
3. Ring topology
4. Mesh topology

1. Bus topology

Bus network is a one-cable topology in which all workstations are connected to a single cable (Linear Bus) that is terminated at each end. All nodes (file servers, work stations and peripherals) are connected to the main cable by drop lines and caps. Signals are broadcasted to all stations, but stations only act on the frames addressed to them. All workstations hear all transmissions on the cable, but select those messages addressed on that particular workstation.



Bus Topology

Advantages

- Initial set-up of a linear bus is easy.
- Easy to connect a computer or peripheral devices.
- More reliable from hardware point of view.
- Easy to extend since new nodes can be easily connected as the workload grows.

- Coverage area can be increased by using repeaters.

Disadvantages

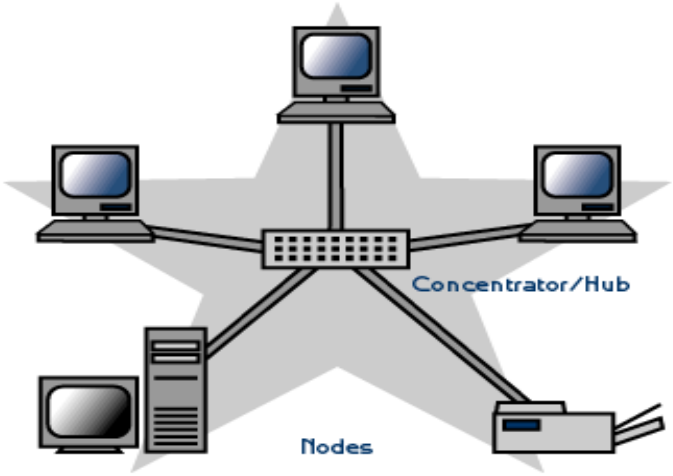
- The primary disadvantage is that a break in the cable affects the entire LAN.
- Fault diagnosis is difficult since detection of fault may have tobe performed from many points.
- The nodes must be intelligent for working of the protocols.
- Terminators are required at both ends of the backbone cable.

2. Star Topology

In a star network each workstation is connected to a single central controller called the hub or a switch or a concentrator using a separate cable. Data on a star network passes through the central controller before reaching at its destination. The central controller manages all the functions of the network. It acts as a repeater for the data flow.

Advantages

- Easy to install and ware.
- It takes less cable than the mesh networks.
- A link failure does not affect the entire network.
- Nodes can be added and removed without affecting the network.
- Easy to detect faults and remove parts.



Star Topology

Disadvantages

- Requires more cable than the bus topology.
- If the central controller fails the entire network fails.
- Limited number of nodes can be installed in the network.
- More expensive than linear bus topologies because of the cost of the hubs or concentrator.

3. Ring Topology

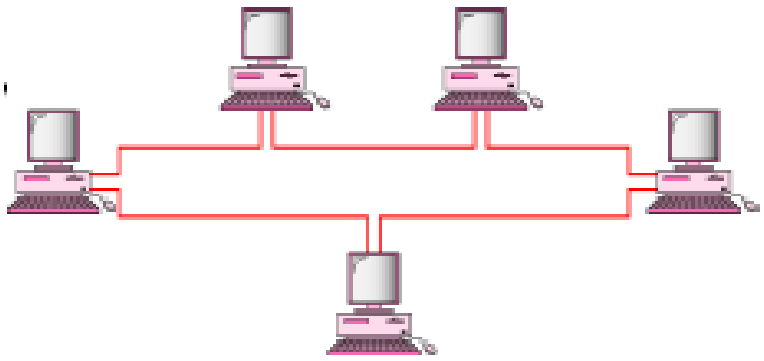
A ring network is a closed loop of cables. Each workstation is connected to two other workstations, one that precedes it and one that succeeds it, forming a loop or ring. Data is sent from workstation to workstation around the ring in the same direction, passing through workstations until it reaches its destination. Each workstation acts as a repeater, resending the message to the next workstation. The response time of a ring is determined by the number of workstations, i.e. the more workstations, the slower the LAN.

Advantages

- Ring topology uses less cabling.
- Performs better than star topology under heavy network load.

Disadvantages

- The main disadvantage is that a cable break between devices affects the entire LAN.
- The ring topology usually demands higher implementation cost because the token ring network adopter cards are more costly than the Ethernet cards.



Ring Topology

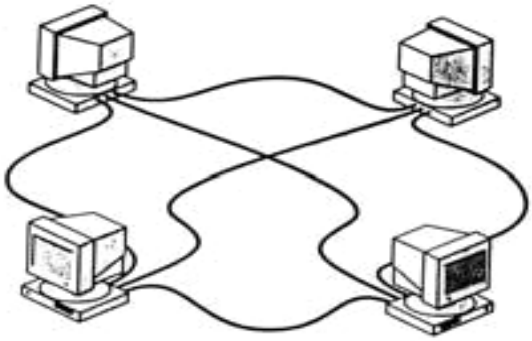
4. Mesh Topology

In a mesh topology, each computer is connected to every other computer by dedicated point-to point link. A fully connected mesh network has n× (n-1) cable links to connect n devices. So each node or device must have (n-1) connection points.

Advantages

- Use of dedicated link eliminates the traffic problem
- Easy to detect fault and isolate fault

- Robust since failure of one link does not affect other.
- Provides security and privacy



Mesh Topology

Disadvantages

- This configuration provides redundant paths throughout the network
- These networks are expensive to install because they use a lot of cabling.
- Number of input/output port is too high.

1.7.3 Comparison of network topologies

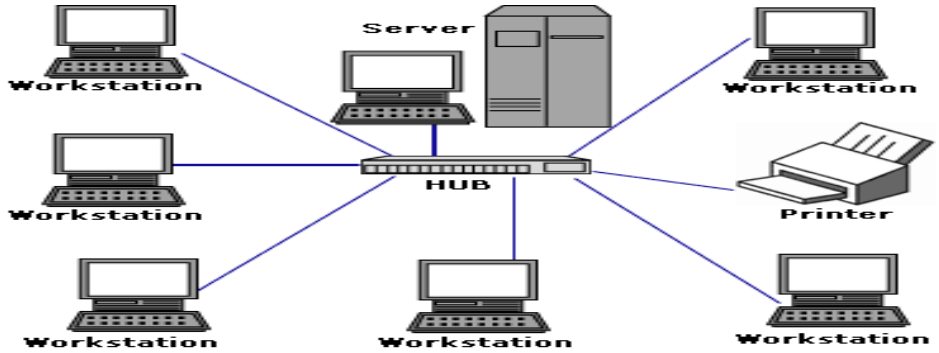
Topology	Use	Pros	Cons
Bus	Central logical topology for Ethernet	• Ease of initial set-up • Low implementation costs	• Cable breaks affect the entire network
Star	Central physical topology for various logical implementation	• Cable break usually affects only one workstation • Workstations can be added easily, without affecting the entire network	• Excessive cable cost due to distance factor
Ring	Central logical topology for Token Ring and FDDI	• Uses less cabling	• Cable breaks between devices or node failure affect the entire network • Higher implementation costs
Mesh	Point-to-Point topology	• Uses more cabling	• Robust

1.8 Categories of Networks

Networks are categorized on the basis of their geographical coverage. The three basic categories of computer networks based on the coverage distance are explained as follows:

1.8.1 Local Area Networks (LAN)

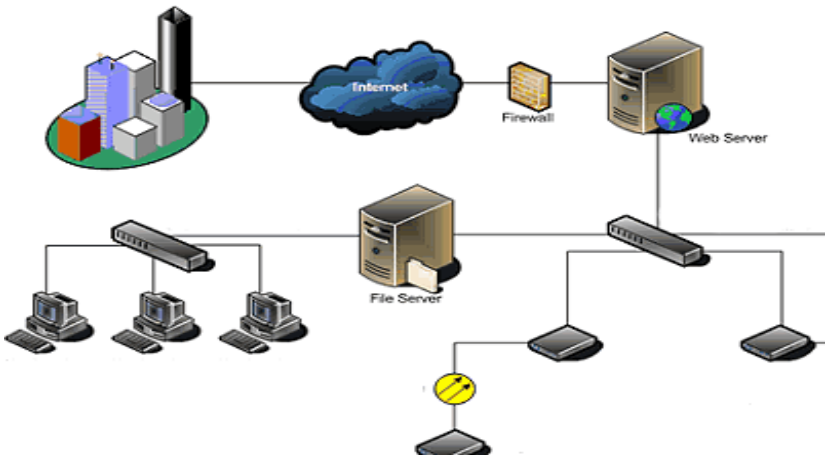
These are small computer networks that are confined to a localizedarea. It could be a network inside an office on one of the floor of a building or a LAN could be a network consisting of the computers in an entire building.



The main purpose of a LAN is resources sharing.As in the above figure the work stations of a LAN can share the files in the server and share the printer. These are privately owned networks controlled and managed by the single organization or person. They use the connectivity technologies, primarily Ethernet and Token Ring.

1.8.2 Metropolitan Area Network (MAN)

A MAN connects multiple geographically nearby LANs to one another within a cities or a metropolis.



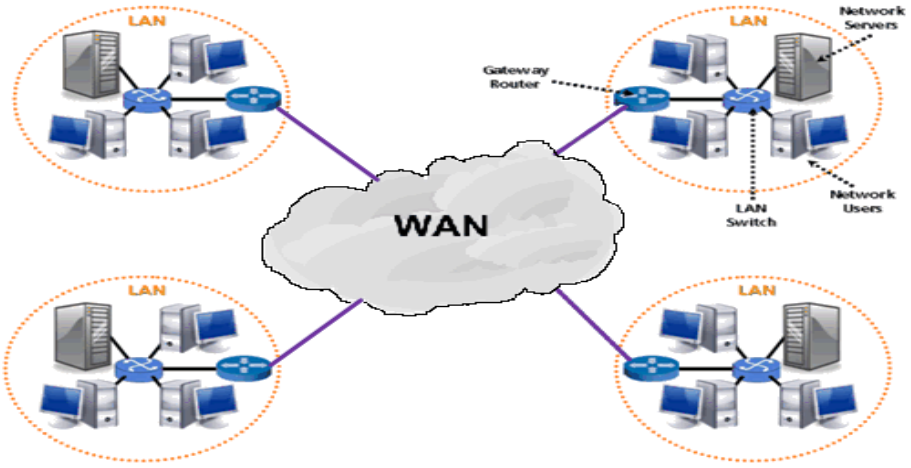
Metropolitan Area Network

The typical size of MAN lies between the size of LANs and WANs.
A MAN is made from switches and routers connected to one another with high speed links, usually fiber optic cables. Thus a MAN lets two remote nodes communicate as if they were part of the same local area network.

1.8.3 Wide Area Network (WAN)

As the name implies, WAN spans large geographically spread area. A **WAN** in comparison is not restricted to a limited geographical location, although it might be confined within the bounds of a state or country.

For example, the network in the entire state of Odisha could be a WAN. A WAN is a geographically dispersed collection of LANs. A network device called a Router or a Gateway connects a LAN to a WAN. The router maintains the addresses of LANs and WANs.



Wide Area Network

A WAN may be owned by a corporation or a public organization and accessible to the public. The technology offers high speed data communication and relatively expensive. The Internet is an example of a worldwide public WAN.

1.8.4 Performance comparisons of LAN and WAN

Performances of a typical LAN and a WAN are summarized in the following table.

Table: Comparison of LAN and WAN

Category	LAN	WAN
Definition	LAN is a computer network covering a small geographic area like a home, office, institutions,	WAN is a computer network that covers a large geographical area such as a state, countries

	or a group of buildings.	and continents.
Ownership	Complete ownership by a single organization or a person	Not owned by any single organization, rather exist under distributed ownership.
Setup cost	Setup cost is lower in comparison.	Initial setup cost is high.
Data Transfer rate	LANs have high data transfer rate	WANs have lower data transfer rate.
Error rate	LANs provide low error rates	WANs provide high error rate
Maintenance	Maintenance of a LAN is easy and cheaper.	Maintenance of a WAN is difficult and costly.
Technology	LANs primarily use Ethernet, Token Ring.	WAN technologies include X.25 ATM and Frame Relay

1.9 Protocols

A Protocol is defined as a set of rules that governs data communications. It is one of the important components of a data communications system.

A network protocol defines what is to be communicated, how it is to be communicated and when it is to be communicated. It include mechanisms for devices to identify and make connections with each other as well as the rules that specify how data are packaged in to messages sent and received.

When the sender sends a message it may consist of text, number, images, etc. which are converted into bits and grouped into blocks to be transmitted and often certain additional information called control information is also added to help the receiver interpret the data.

1.9.1 Elements of a Protocol

There are three key elements of a protocol:

1. Syntax

It means the structure or format of the data.

It is the arrangement of data in a particular order.

2. Semantics

It tells the meaning of each section of bits and indicates the interpretation of each section.

It also tells what action/decision is to be taken based on the interpretation.

3. Timing

It tells the sender about the readiness of the receiver to receive the data

It tells the sender at what rate the data should be sent to the receiver to avoid overwhelming the receiver.

1.10 Standards in networking

Standards are necessary in networking to ensure interconnectivity and interoperability between various networking hardware and software components.

Without standards we would have proprietary products creating isolated islands of users which cannot interconnect.

1.10.1 Concept of Standard

Standards provide guidelines to product manufacturers, vendors, government agencies and other service providers to ensure national as well as international interconnectivity and communication.

Data communications standards are classified into two categories:

1. De facto Standard

These are the standards that have been traditionally used and mean by **fact** or **by convention**

These standards are not approved by any organized body but are adopted by widespread use.

These standards established originally by manufacturers that seek to define the functionality of a new product or technology.

2. De jure standard

It means by **law** or **by regulation.** These standards are legislated and approved by a body that is officially recognized.

1.10.2 Standard Organizations in field of Networking

Standards are created by standards creation committees, forums, and government regulatory agencies.

Examples of Standard Creation Committees:

1. International Organization for Standardization (ISO)
2. International Telecommunications Union – Telecommunications Standard (ITU-T)
3. American National Standards Institute (ANSI)
4. Institute of Electrical & Electronics Engineers (IEEE)
5. Electronic Industries Associates (EIA)

Examples of Forums

1. ATM Forum & ATM Consortium
2. Frame Relay Forum
3. Internet Engineering Task Force(IETF)

Examples of Regulatory Agencies:

Federal Communications Committee (FCC) is the government regulatory body in U.S for all communication technology.

1.11Key terms & Concepts

- **Data communication** is the transfer of data or information from a source to a destination.
- **Data communication system** is made up of hardware and software that ensures transmission of data in an accurate and timely manner.
- **Data flow** between the two devices can be in simplex, half duplex and full duplex modes.
- **Computer Network** is an interconnection of autonomous computers and other devices that use a common network language to share the network resources.
- **Topology** of a network describes the layout or appearance of a network that is how the computers, cables, and other components are connected**.**
- **LAN** is a data communication system within abuilding, or campus or between nearby building
- **MAN** is a data communication system covering an area of the entire town or city.
- **WAN** is adata communication system spanning states, countries or the whole world.
- **Protocol** is a set of rules that govern data communication; the key elements of a protocol are syntax,semantics, and timing.
- **Standards** are necessary to ensure that products from different manufacturers can work together as expected.

1.12 Self Assessment Questions

1.12.1 Short answer type questions

1. What are the characteristics of data communication?
2. List out five components of data communications system.
3. What are the three modes of data transmission?
4. Define a computer network.
5. What are the network performance criteria?
6. Define transit time and response time.
7. Differentiate half duplex and full duplex communication.
8. Suggest two points to improve the performance of network.

9. What are the two ways in which devices in a network can be connected?
10. What is the basic purpose of setting up a LAN?
11. Suppose we have to add new nodes to the network, then which is the best suited topology and why?
12. What is the main drawback of a star topology?
13. If n numbers of devices to be connected, how many cable links are required for a mesh, ring, and star topology?
14. What do you mean by reliability of a computer network?
15. What are different categories of standards?

16. 1.12.2 Long answer type questions

1. Draw the block diagram for the data communication system. Explain each of its components.
2. What are the basic network topologies? Write the features, advantages and disadvantages of Star and Bus topology.
3. Differentiate between the two categories of networks LAN and WAN.
4. What is a protocol? What are the key elements of a protocol? Why is it necessary for data communications?
5. Why standards are needed? What are two categories of standards? Name five standard organizations in the field of data communication and networks.

1.13 References& Suggested Readings

1. Behrouz A. **Forouzan**, "*Introduction to Data Communications and Networking***",** McGraw-Hill Education (India), New Delhi.
2. Andrew S. **Tanenbaum**, "*Computer Networks*", PHI Learning Pvt. Ltd
3. James F. **Kurose,** Keith W. **Ross**, "*Computer Networking: A Top-Down Approach Featuring the Internet*", Pearson Education Inc., New Delhi.
4. Wayne **Tomasi,** "*Introduction to Data Communications and Networking*", Pearson Education Inc., New Delhi.
5. L. L. **Peterson** and B. S. **Davie**," *Computer Networks*", Elsevier Inc,

Unit – 2
Network Reference Models

Structure

2.0 Introduction

Data communication can take place between two devices if they agree to a set of common rules called protocol. Protocols guide the interconnection between two heterogeneous elements of a large network and the standards are needed for interoperability of different elements of data communication between two parties. A network reference model, therefore, defines standards for the communicating hosts. The operation of a computer network is guided by the network reference models. This unit gives the understanding in working of the most important OSI and TCP/IP reference model.

2.1 Objectives

At the end of this unit, you will be able to:

- Understand the need for network reference models
- Identify the benefits of layered architecture of the network models.
- List seven layers of the OSI reference model
- Know the working of OSI layers and their services.
- List the functions and responsibilities of the layers of OSI model
- Know the working of TCP/IP layers and their services.
- List the functions and responsibilities of the layers of TCP/IP model
- Summarize the roles of OSI layers and compare with that of TCP/IP layers.

2.2 Network Model

A network model is a design of a computer network that includes the hardware, software, access methods and protocols. A Network model provides only a conceptual framework for communications between computers. It typically has a layered structure.

2.2.1 Layered Architecture of Network Model

The communication between two parties in a computer network involves a layered structure and each corresponding layers have similar functions at the both sender and receivers and a particular common language is used for conversation called protocol.

Benefits of Layered Architecture

The layering architecture provides the following benefits

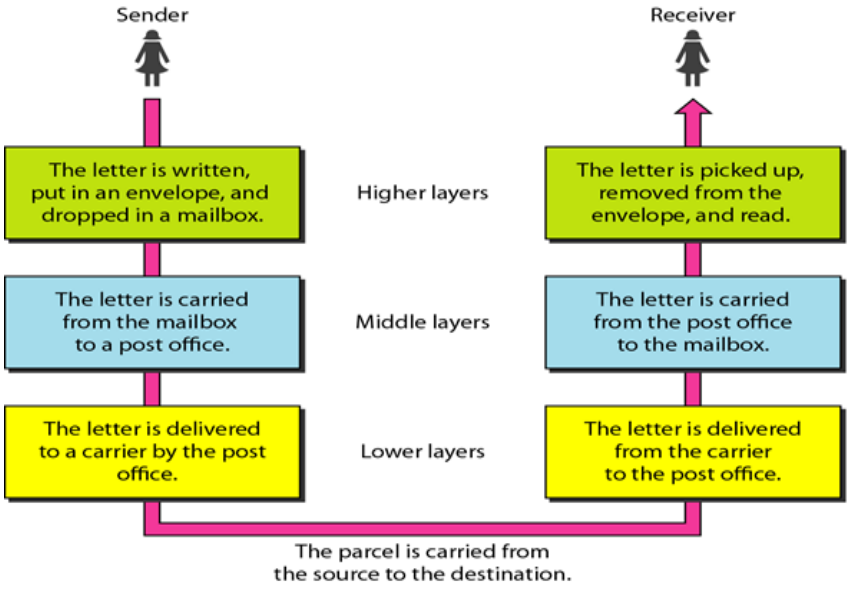
- Layer architecture simplifies the network design.
- It is easy to debug network applications
- The network management is easier due to the layered architecture.

- Network layers follow a set of rules, called protocol.
- The protocol defines the format of the data being exchanged, and the control and timing for the handshake between layers

Layered Task

The main objective of a computer network is to be able to transfer the data from sender to receiver. This task can be done by breaking it into small sub tasks, each of which is well defined. Each subtask will have its own process or processes to do and will take specific inputs and give specific outputs to the subtask before or after it. In more technical terms we can call these sub tasks as layers. In general, every task or job can be done by dividing it into sub task or layers.

To explain the need for layering and a common language called protocols for communication between two parties in network architecture, we take an analogy in our daily life. Consider two friends who communicate through postal mail in a step by step manner. We depict the following picture to explain the scenario.



Example of Layered Task

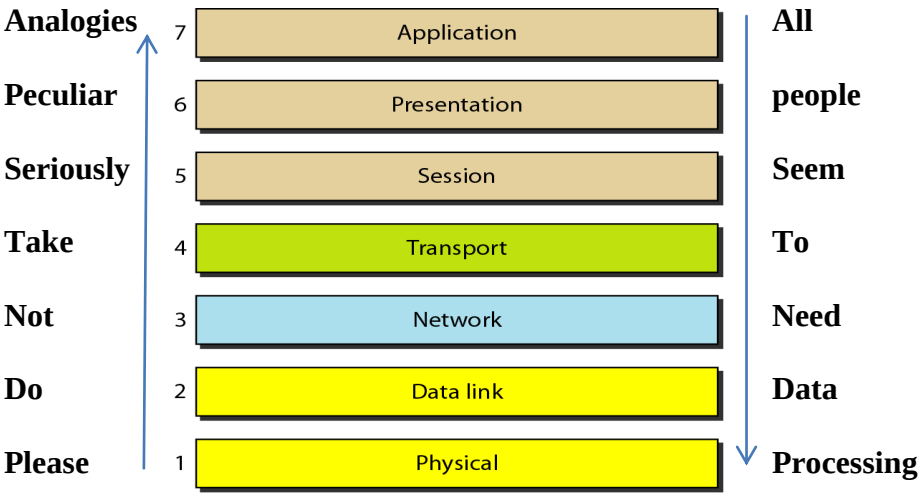
2.3 Open Systems Interconnection (OSI) Reference Model

- The model was developed by the International Organisation for Standardisation (ISO) in 1984. It is now considered the primary architectural model for inter-computer communications.
- The model is a descriptive network scheme. It ensures greater compatibility and interoperability between various types of network technologies.

- It describes how information or data makes its way from application programmes through a network medium to another application programme located on another network.
- The model divides the problem of moving information between computers over a network medium into seven smaller and more manageable problems.

2.3.1 Seven Layers of OSI Model

It is a hierarchical model that groups its processes into layers. It has 7 layers as in the following figure. We use the mnemonics of the initial letters to remember the seven layers of the OSI model. The mnemonics are: "Please Do Not Take Seriously Peculiar Analogies" and "All People Seem to Need Data Processing**"**.



Seven layers of OSI Model

- The OSI Reference Model is composed of seven layers, each specifying particular network functions.
- Each layer provides a service to the layer above it in the protocol specification. The lower 4 layers (transport, network, data link and physical —Layers 4, 3, 2, and 1) are concerned with the flow of data from end to end through the network.
- The upper four layers of the OSI model (application, presentation and session—Layers 7, 6 and 5) are orientated more towards services to the applications.

The lower two OSI model layers are implemented with hardware and software. The upper five are generally implemented only in software.

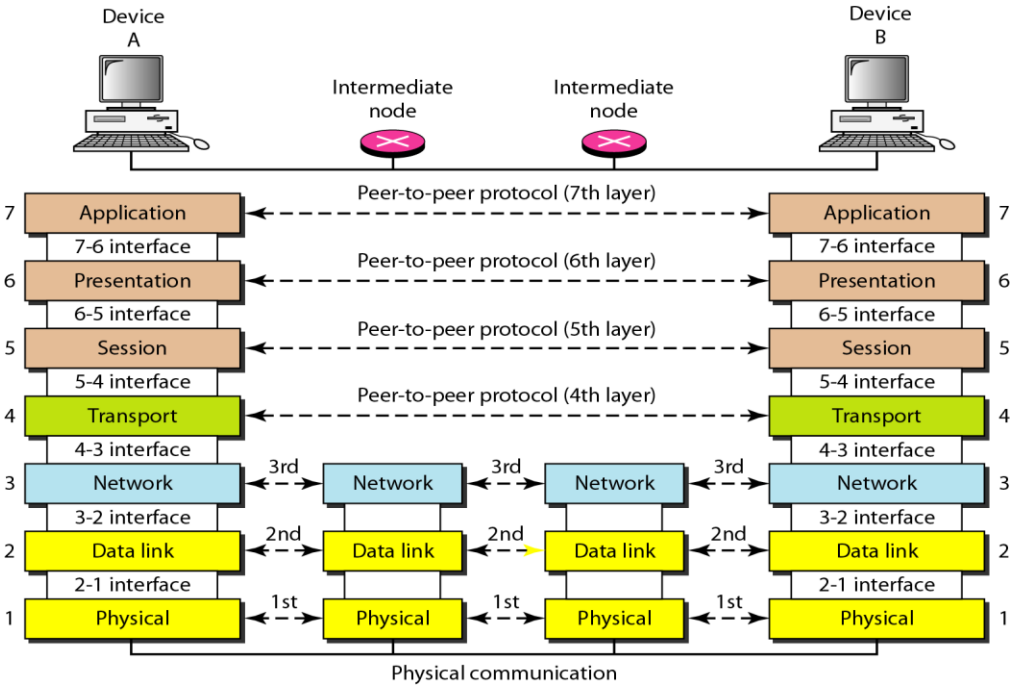
2.3.2 Communications & Interfaces

For communication to occur, each layer in the sending device adds its own information to the message it receives from the layer just above it and passes the whole package to the layer just below it. Each layer in the receiving device removes the information added at the corresponding layer and sends the obtained data to the layer above it.

Every Layer has its own dedicated function or services and is different from the function of the other layers. On every sending device, each layer calls upon the service offered by the layer below it. On every receiving device, each layer calls upon the service offered by the layer above it. Between two devices, the layers at corresponding levels communicate with each other .i.e layer 2 at receiving end can communicate and understand data from layer 2 of sending end. This is called peer –to – peer communication.

For this communication to be possible between every two adjacent layers there is an interface. An interface defines the service that a layer must provide. Every layer has an interface to the layer above and below it.

The following figure depicts communication between machines as a peer-to-peer process using protocols appropriate to a given layer and the interfaces between layers.

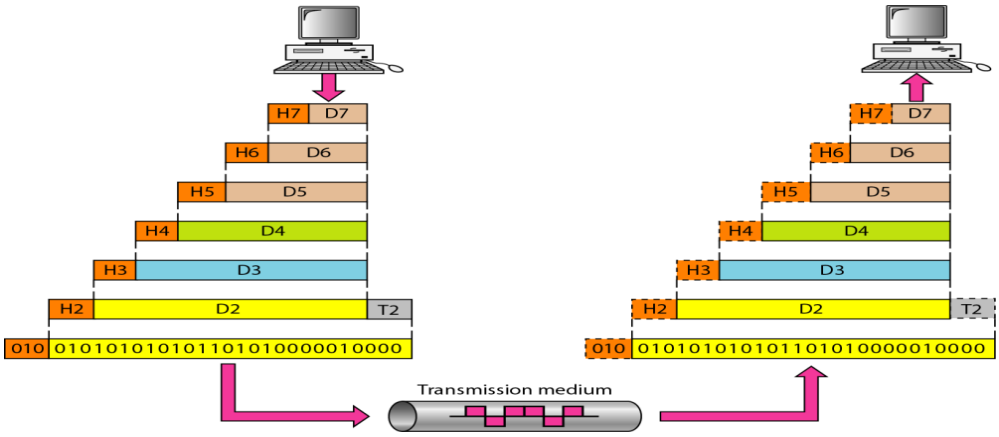


Peer-to-peer communication architecture

2.3.3 Encapsulations and de-capsulation

The process of adding the header before the data and tailor after the data at the sender is called encapsulation. On the other hand the process of removing

the header and trailer by the corresponding layer is called de-capsulation. It is the data link layer which adds the trailer also to the data frame.



Encapsulation and De-capsulation

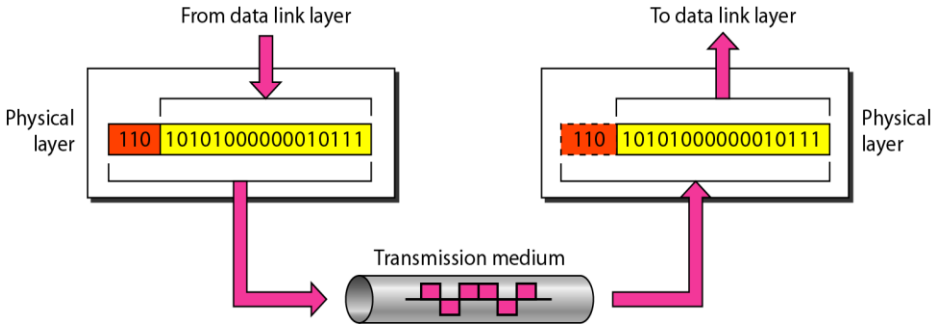
2.3.4 Functions and Responsibilities OSI Layers

The specific functions and responsibilities of each layer are listed as follows.

1. Physical Layer

The physical layer coordinates the functions required to transmit a bit stream over a physical medium. It also defines the procedures and functions that physical devices and interfaces have to perform for transmission occur. The physical layer is concerned with the following functions:

- **Physical characteristics of interfaces and media:** The physical layer defines the characteristics of the interface between devices and the transmission media, including its type.
- **Data rate:** The physical layer defines the transmission rate, the number of bits sent each
- **Representation of the bits**: The physical layer data consist of a stream of bits without any interpretation. To be transmitted**,** bits must be encoded into signals –electrical or optical-. The physical layer defines the type of encoding.



- **Line configuration**: the physical layer is concerned with the connection of devices to the medium.

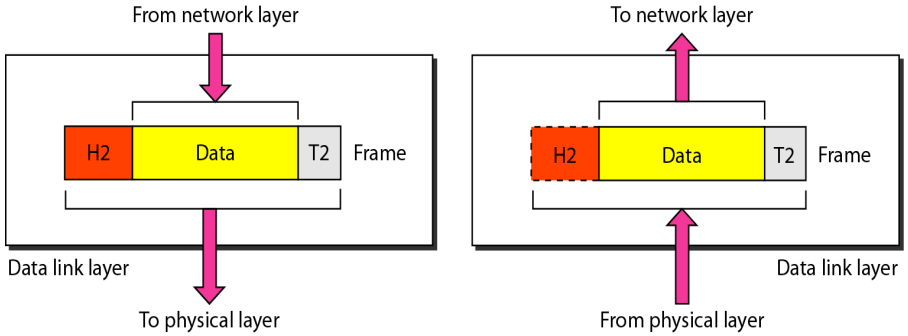
- **Physical topology**: The Physical layer is responsible for defining the physical layout called topology of the underlying network such as star, ring, bus, mesh and tree topology.
- **Transmission Mode**: The physical layer is also responsible for defining the transmission mode such as, simplex, half duplex, full duplex mode.

Main responsibility of the physical layer is transmission of bits from one hop to the next.

2. Data Link Layer

The data link layer transforms the physical layer, a raw transmission facility, to a reliable link and is responsible for node-to-node delivery. The data link layer performs the following functions.

- **Framing:** The data link layer divides the stream of bits received from the network layer into data units called frames.
- **Physical addressing:** If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the physical address of the sender and receiver of the frame.



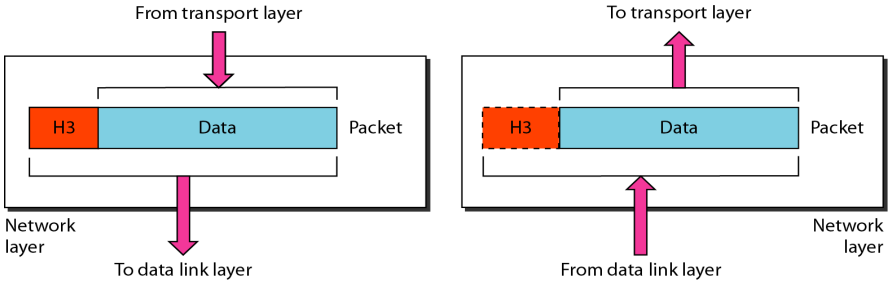
- **Flow Control**: If the rate at which the data are absorbed by the receiver is less than the rate produced in the sender, the data link layer imposes a flow control mechanism to prevent overwhelming the receiver.
- **Error control**. The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. Error control is normally achieved through a trailer to the end of the frame.
- **Access Control.** When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any time.

The main responsibility of the data link layer is hop to hop transmission of frames.

3. Network Layer

The Network layer is responsible for the source-to-destination delivery of a packet possible across multiple networks. The network layer is responsible for the following functions.

- **Logical addressing**. The physical addressing implemented by the data link layer handles the addressing problem locally.
- The network layer adds a header to the packet coming from the upper layer, among other things, includes the logical address of the sender and receiver.

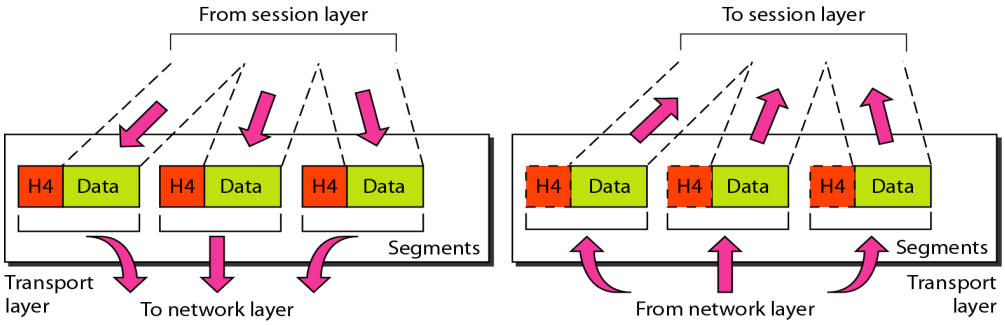


- **Routing**. When independent networks or links are connected together to create an internetwork (a network of networks) or a large network, the connecting devices (called routers or gateways) route or switch the packets to their final destination.

The main responsibility of Network Layer is transmission of packets from source to destination

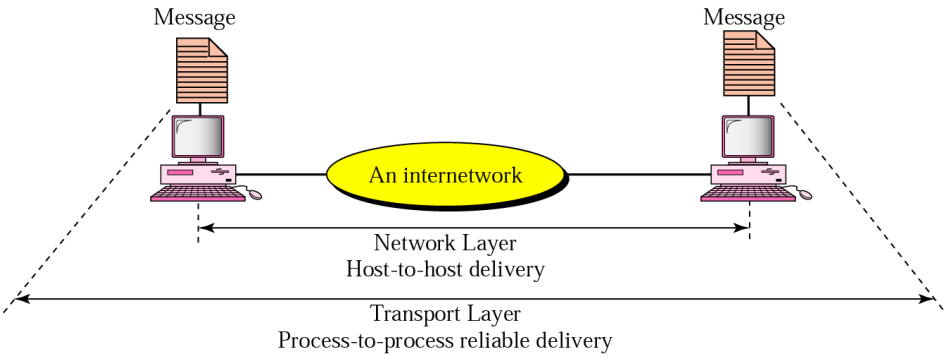
4. Transport Layer

The transport layer is responsible for process-to-process delivery of the entire message. The network layer oversees host-to-destination delivery of individual packets; it does not recognize any relationship between those packets.



The specific functions of the transport layer include:

- **Port addressing**: computer often run several processes (running programs) at the same time. Process-to-process delivery means delivery from a specific process on one computer to a specific process on the other.
- **Process-to-process delivery**: The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.



- **Segmentation and reassembly**: a message is divided into transmittable segments, each having a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arrival at the destination.

  Connection control: The transport layer can be either connectionless or connection-oriented
- **Flow control**: the transport layer performs a flow control end to end. The data link layer performs flow control across a single link.
- **Error control**: the transport layer performs error control end to end. The data link layer performs control across a single link.

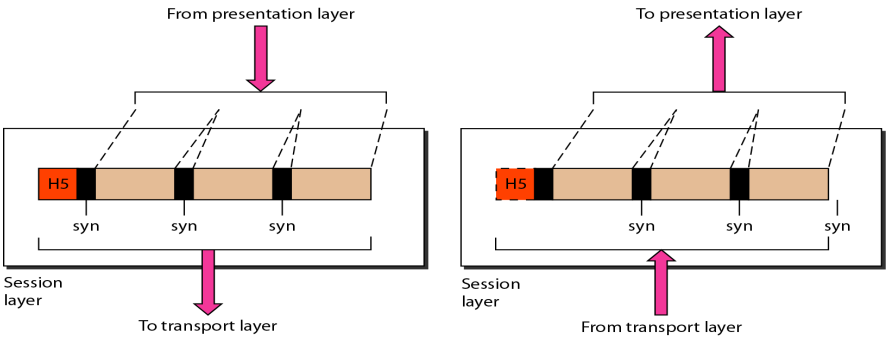
The main responsibility of the transport layer is process to process delivery of the entire message

5. The Session Layer

The session layer allows two applications on separate computers to set up use and terminate a connection called a session. The session layer is the network dialog controller.

The specific functions of the session layer are:

- **Dialog control**: Allows communication either in half-duplex or full-duplex mode.
- **Synchronization**: Add check points to the stream of data for acknowledgement and synchronization between sender and the receiver.

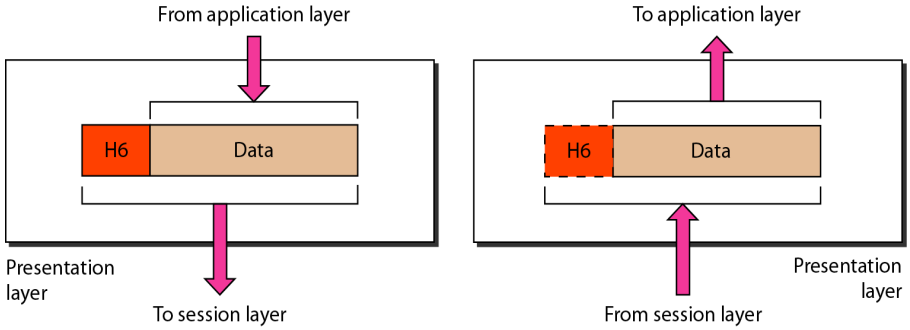


Main responsibility of session layer is dialog control and synchronization

6. Presentation Layer

The presentation layer is concerned with syntax and semantics of the information exchanged between the two systems. It carries out the functions like:

- Protocol conversion
- Data translation
- Encryption and decryption
- Compression and
- Decompression

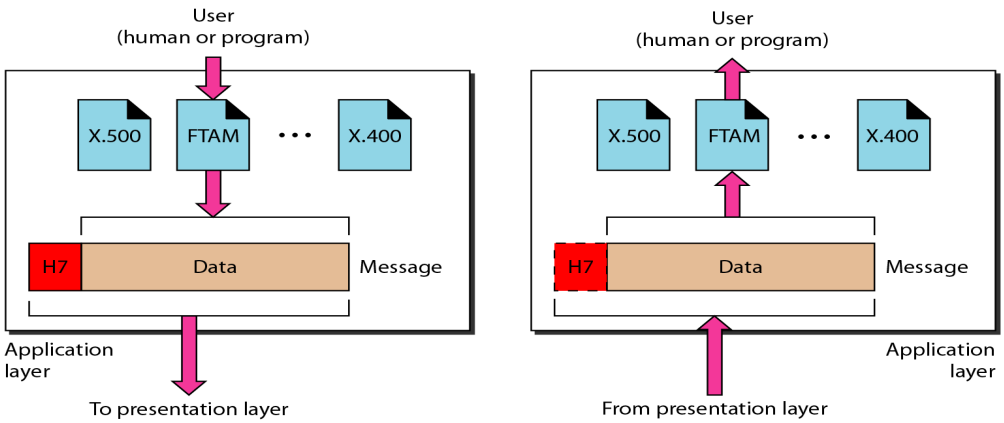


The main responsibility of the Presentation layer is translation, compression and encryption

7. Application Layer

The application layer enables the user to access the network services. It provides user interfaces and support for network services such as:

- Electronic email
- Remote login using TELNET
- File transfer through FTP
- Web services through WWW
- Directory services and so on.

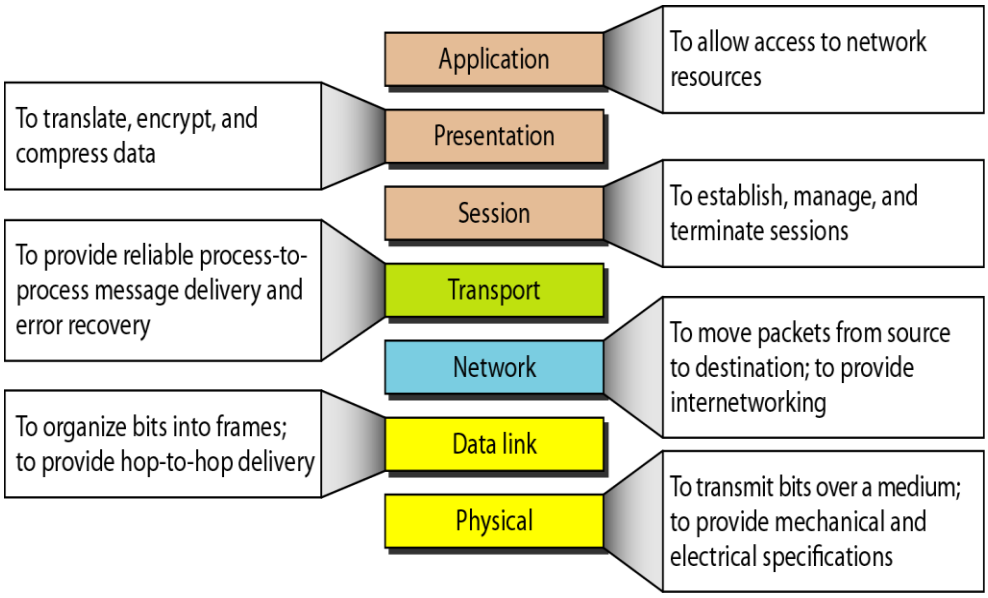


- **X500** is a directory service used to provide information and access to distributed objects
- **X400** is services that provides basis for mail storage and forwarding
- **FTAM (File transfer, access and management)** provides access to files stored on remote computers and mechanism for transfer and manage them locally.

Main Responsibility of application layer is to provide access to network resources.

2.3.4 Summary of OSI Layers functions

We use the pictorial presentation that summarizes the functions performed by various layers by communication between two users over the transmission medium. The following figure shows the main functions of each layers of OSI reference model.

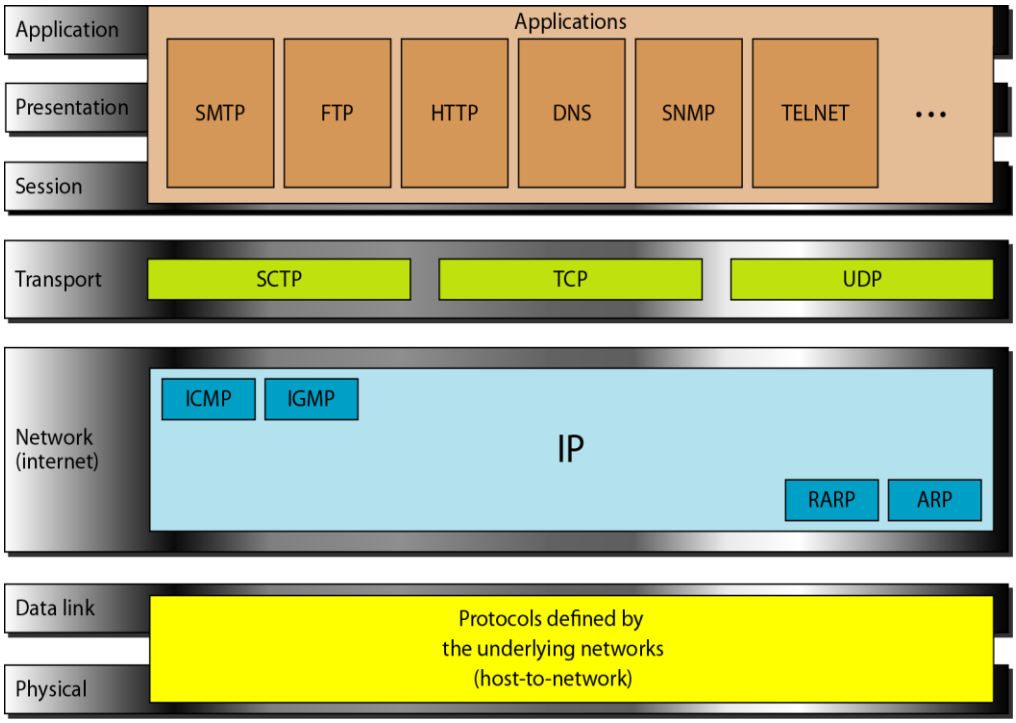


2.4 TCP/IP Model

It is also called as the TCP/IP protocol suite. It is a collection of protocols. There are multiple layers and higher layer protocols are supported by lower layer protocols. Originally the model had four layers:

1. Host to Network Layer
2. Internet Layer
3. Transport Layer
4. Application Layer

The figure below shows the comparison of OSI model and TCP/IP model along with the protocols.



Comparison of OSI model and TCP/IP model

The structure TCP/IP model is very similar to the structure of the OSI reference model. The OSI model has seven layers where the TCP/IP model has four layers.

The Application layer of TCP/IP model corresponds to the Session, Presentation & Application Layer of OSI model.

The Transport layer of TCP/IP model corresponds to the Transport Layer of OSI model

The Network layer of TCP/IP model corresponds to the Network Layer of OSI model

The Host to network layer of TCP/IP model corresponds to the Physical and Data link Layer of OSI model.

2.4.1 Functions of the Layers of TCP/IP Model

1. Host to Network Layer

- This layer is a combination of protocols at the physical and data link layers. It supports all standard protocols used at these layers.

2. Network Layer

- It is also called as the Internetwork Layer. It holds the Internetworking Protocol (IP) which is responsible for source to destination transmission of data.
- The Internetworking Protocol (IP) is a **connection-less** &**unreliable protocol.**
- It is a best effort delivery service. i.e. there is no error checking in IP, it simply sends the data and relies on its underlying layers to get the data transmitted to the destination.
- IP transports data by dividing it into **packets or datagrams** of same size. Each packet is independent of the other and can be transported across different routes and can arrive out of order at the receiver.
- In other words, since there is no connection set up between the sender and the receiver the packets find the best possible path and reach the destination. Hence, the word **connection-less**.
- The packets may get dropped during transmission along various routes. Since IP does not make any guarantee about the delivery of the data its call an **unreliable** protocol.
- Even if it is unreliable IP cannot be considered weak and useless; since it provides only the functionality that is required for transmitting data thereby giving maximum efficiency. Since there is no mechanism of error detection or correction in IP, there will be no delay introduced on a medium where there is no error at all.
- Including IP, Network layer is associated with other four protocols:
    i. ARP
    ii. RARP
    iii. ICMP
    iv. IGMP

I. ARP – Address Resolution Protocol

- It is used to resolve the physical address of a device on a network, where its logical address is known.
- Physical address is the 48 bit address that is imprinted on the NIC or LAN card, Logical address is the Internet Address or commonly known as IP address that is used to uniquely & universally identify a device.

II. RARP– Reverse Address Resolution Protocol

It is used by a device on the network to find its Internet address when it knows its physical address.

III. ICMP- Internet Control Message Protocol

- It is a signaling mechanism used to inform the sender about datagram problems that occur during transit.
- It is used by intermediate devices.
- In case and intermediate device like a gateway encounters any problem like a corrupt datagram it may use ICMP to send a message to the sender of the datagram.

IV. IGMP- Internet Group Message Protocol

It is a mechanism that allows sending the same message to a group of recipients.

3. Transport Layer

Transport layer protocols are responsible for transmission of data running on a process of one machine to the correct process running on another machine. The transport layer contains three protocols:

I. TCP
II. UDP
III. SCTP

I. TCP – Transmission Control Protocol

- TCP is a reliable connection-oriented, reliable protocol. i.e. a connection is established between the sender and receiver before the data can be transmitted.
- II. It divides the data it receives from the upper layer into segments and tags a sequence number to each segment which is used at the receiving end for reordering of data.

II. UDP – User Datagram Protocol

- UDP is a simple protocol used for process to process transmission.
- It is an unreliable, connectionless protocol for applications that do not require flow control or error control.
- It simply adds port address, checksum and length information to the data it receives from the upper layer.

III. SCTP – Stream Control Transmission Protocol

- SCTP is a relatively new protocol added to the transport layer of TCP/IP protocol suite.
- It combines the features of TCP and UDP.
- It is used in applications like voice over Internet and has a much broader range of applications

4. Application Layer

The Application Layer is a combination of Session, Presentation & Application Layers of OSI models and defines high level protocols like File Transfer (FTP), Electronic Mail (SMTP), Virtual Terminal (TELNET), Domain Name Service (DNS) etc.

2.5 Addressing in TCP/IP

The TCP/IP protocol suited involves 4 different types of addressing:

1. Physical Address
2. Logical Address
3. Port Address
4. Specific Address

1. Physical Address

- Physical Address is the lowest level of addressing, also known as link address.
- It is local to the network to which the device is connected and unique inside it.
- The physical address is usually included in the frame and is used at the data link layer.
- Physical address also called MAC address that is 6 byte (48 bit) in size and is imprinted on the Network Interface Card (NIC) of the device.
- The size of physical address may change depending on the type of network. Ex. An Ethernet network uses a 6 byte MAC address.

2. Logical Address

- Logical Addresses are used for universal communication.
- Most of the times the data has to pass through different networks; since physical addresses are local to the network there is a possibility that they may be duplicated across multiples networks also the type of physical address being used may change with the type of network encountered.
- For example, Ethernet to wireless to fiber optic. Hence physical addresses are inadequate for source to destination delivery of data in an internetwork environment.
- Logical Address is also called as IP Address (Internet Protocol address).
- At the network layer, device i.e. computers and routers are identified universally by their IP Address.
- IP addresses are universally unique.
- Currently there are two versions of IP addresses being used:
  a. **IPv4**: 32 bit address
  b. **IPv6:** 128 bit address

3. Port Address

A logical address facilitates the transmission of data from source to destination device. But the source and the destination both may be having multiple processes communicating with each other.

Example: Users A & B are chatting with each other using Google Talk; Users B & C are exchanging emails using Hotmail. The IP address will enable transmitting data from A to B, but still the data needs to be delivered to the correct process. The data from A cannot be given to B on yahoo messenger since A & B are communicating using Google Talk.

Since the responsibility of the IP address is over here there is a need of addressing that helps identify the source and destination processes. In other words, data needs to be delivered not only on the correct device but also on the correct process on the correct device. A Port Address is the name or label given to a process. It is a 16 bit address. Ex. TELNET uses port address 23, HTTP uses port address 80.

4. Specific Address

Port addresses address facilitates the transmission of data from process to process but still there may be a problem with data delivery.

Example: Consider users A, B & C chatting with each other using Google Talk. Every user has two windows open, user A has two chat windows for B & C, user B has two chat windows for A & C and so on for user C Now a port address will enable delivery of data from user A to the correct process (in this case Google Talk) on user B but now there are two windows of Google Talk for user A & C available on B where the data can be delivered.

Again the responsibility of the port address is over here and there is a need of addressing that helps identify the different instances of the same process. Such addresses are user friendly addresses and are called specific addresses.

Example: Multiple Tabs or windows of a web browser work under the same process that is HTTP but are identified using **Uniform Resource Locators (URL**).

2.6 Key terms & Concepts

- **A network model** is a design of a computer network that includes the hardware, software, access methods and protocols.
- **Network protocols** defines the format of the data being exchanged, and the control and timing for the handshake between layers

- **Open Systems Interconnection (OSI) reference model** was approved as an international standard for communications architecture.
- **TCP/IP Reference Model** is also called as the **TCP/IP protocol suite**.
- The **Internetworking Protocol (IP**) is a **connection-less** &**unreliable protocol**
- **TCP** is a reliable **connection-oriented, reliable protocol**
- **UDP** is an unreliable, connectionless protocol for applications that do not require flow control or error control.
- **Physical address also called MAC address** that is 6 byte (48 bit) in size and is imprinted on the Network Interface Card (NIC) of the device.
- At the network layer each device i.e. computers and routers are identified universally by their **IP Address**
- A **Port Address** is the name or label given to a process. It is a 16 bit address.
- Currently there are two versions of IP addresses being used:
  a. **IPv4**: 32 bit address
  b. **IPv6:** 128 bit address

2.7 Self-Assessment Questions

2.7.1 Short Answer type questions

1. List two advantages of layering principle in computer networks.
2. Distinguish between peer-to-peer relationship and a primary-secondary relationship?
3. Name two similar functions of data link and the transport layer.
4. What is the difference between the physical and logical addressing
5. Which two layers of OSI model are not operative in reality?
6. What is the difference between node-to-node and source-to-destination delivery?
7. Which layer is responsible for routing in an inter-network?
8. Why IP is used even is unreliable?
9. Which layer of the OSI model is called network's dialog controller?

10. Which layer of the OSI model is responsible for process to process delivery of the entire message

2.7.2 Long Answer type questions

1. Explain the encapsulation and de-capsulation process in OSI Model.
2. Differentiate between connectionless and connection oriented operation
3. Explain ISO/ OSI reference model with neat diagram.
4. Compare the layers of OSI Model with that of TCP/IP model.
5. Explain different types of addresses used in TCP/IP

2.8 References and Suggested Readings

1. Behrouz A. **Forouzan**, "*Introduction to Data Communications and Networking***",** McGraw-Hill Education (India), New Delhi.
2. Andrew S. **Tanenbaum**, "*Computer Networks*", PHI Learning Pvt. Ltd
3. James F. **Kurose,** Keith W. **Ross**, "*Computer Networking: A Top-Down Approach Featuring the Internet*", Pearson Education Inc., New Delhi.
4. Wayne **Tomasi,** "*Introduction to Data Communications and Networking*", Pearson Education Inc., New Delhi.
5. L. L. **Peterson** , B. S**. Davie**," *Computer Networks*", Elsevier Inc,

Unit – 3

Transmission Media and Network Devices

Structure

3.0 Introduction

In computer networking, transmission media is a path through which data can travel from a source to the destination. It acts as a data high way. So it is worth understanding the types of media through which data passes and know their characteristics. The devices that inter connect two or more computers and networks are called network devices. In this unit we will describe different types of transmission media and network devices used for data communication and networking.

3.1 Objective

After learning this unit you will be able to:

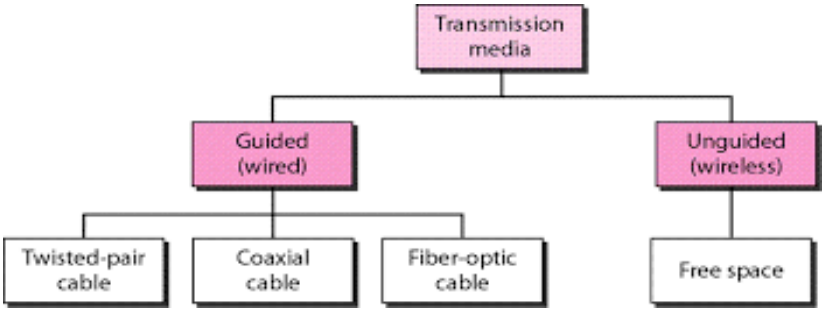
- Define a Transmission Medium
- Know the structure and features, merits and demerits of different types of guided and unguided transmission media.
- Identify different types of cables and their connectivity
- Different ways in which wireless signals are transmitted.
- Identify different types of network devices and their usages

3.2 Transmission Media

A Transmission Medium can be defined as a physical path that can carry information from a source to a destination. The transmission medium can be free space, metallic cables, or fiber-optic cable through which data transmitted in the form of electromagnetic signals.

3.3 Categories of Transmission Media

In data communication, transmission media can be divided into two broad categories, namely, guided and unguided. Guided media include twisted-pair cable, coaxial cable, and fiber-optic cable. Unguided medium is free space.



Categories of Transmission Media

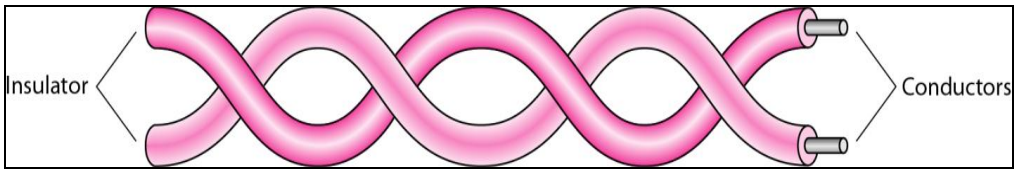
3.4 Guided Media

Guided media provide a conduit from one device to another by physical connection. A signal transmitted along any of these media is directed and contained by the physical medium. Guided media include twisted-pair and coaxial cables those use metallic conductors to accept and transport signals in the form of electric current and Optical fiber cable that accepts and transports signals in the form of light.

3.4.1 Twisted-Pair

Twisted-Pair cable accepts and transports signals in the form of electric current. It consists of two copper conductors, each with its own plastic insulation, twisted together.

One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference. The receiver uses the difference between the two. In addition to the signals sent by the sender, noise and crosstalk may affect both wires and create unwanted signals.



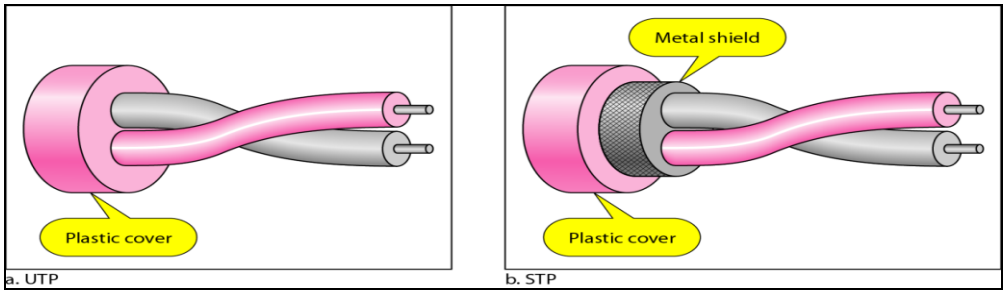
Twisted-pair cable

Twisting makes it probable that both wires are equally affected by external noise. The unwanted signals are mostly canceled out. The number of twists per unit of length has some effect on the quality of the cable.

3.4.1.1 Unshielded vs Shielded Twisted-Pair Cable

The most common twisted-pair cable used in communications is Unshielded Twisted-Pair cable.

Shielded twisted-pair cable has a metal shield or braided-mesh covering that encases each pair of insulated conductors. The figure shows the difference between Unshielded and Shielded Twisted-Pair.



Unshielded and Shielded Twisted-Pair cable

Although metal shield improves the quality of cable by preventing the penetration of noise or crosstalk, it is bulkier and more expensive.

4.1.1.2 Categories of Unshielded Twisted Pair (UTP) cable

The Electronic Industries Association (EIA) has developed standards, to classify Unshielded Twisted-Pair cable into seven categories, suitable for specific uses.

UTP-CAT5e is the most popular UTP cable which came to replace the old coaxial cable that was not able to keep up with the constant growing need for faster and more reliable networks

Category 1/2/3/4/5/6/7 – a specification for the type of copper wire (most telephone and network wire is copper) and jacks. The number (1, 3, 5, etc.) refers to the revision of the specification and in practical terms refers to the number of twists inside the wire (or the quality of connection in a jack).

CAT1 is typically used for telephone wire. CAT1 is used by telco companies providing ISDN and PSTN services.

CAT2, CAT3, CAT4, CAT5/5e, CAT6 & CAT 7 are network wire specifications. This type of wire can support computer network and telephone traffic.

CAT2 is used mostly for token ring networks, supporting speeds up to 4 Mbps. For higher network speeds (100 Mbps or higher) CAT5e must be used, but for the almost extinct 10 Mbps speed requirements, CAT3 will suffice.

CAT3, CAT4 and CAT5 cables are actually 4 pairs of twisted copper wires and CAT5 has more twists per inch than CAT3 therefore can run at higher speeds and greater lengths. The "twist" effect of each pair in the cables ensures any interference presented/picked up on one cable is cancelled out by the cable's partner which twists around the initial cable.

CAT3 and CAT4 are both used for Token Ring networks, where CAT 3 can provide support of a maximum 10Mbps, while CAT4 pushed the limit up to 16Mbps. Both categories have a limit of 100 meters.

The more popular CAT5 wire was later on replaced by the CAT5e specification which provides improved crosstalk specification, allowing it to support speeds of up to 1Gbps. CAT5e is the most widely used cabling specification world-wide.

CAT6 wire was originally designed to support gigabit Ethernet, although there are standards that will allow gigabit transmission over CAT5e wire. It is similar to CAT5e wire, but contains a physical separator between the four pairs to further reduce electromagnetic interference. CAT6 is able to support

speeds of 1Gbps for lengths of up to 100 meters, and 10Gbps is also supported for lengths of up to 55 meters.

CAT7 is a newer copper cable specification designed to support speeds of 10Gbps at lengths of up to 100 meters. To achieve this, the cable features four individually shielded pairs plus an additional cable shield to protect the signals from crosstalk and electromagnetic interference.

3.4.1.2 Unshielded Twisted-Pair Connector

The most common Unshielded Twisted-Pair connector is RJ45. RJ stands for registered jack.
Inside the Ethernet cable, there are 8 color coded wires, with all eight pins used as conductors. These wires are twisted into 4 pairs and each pair has a common color theme. RJ45 specifies the physical male and female connectors as well as the pin assignments of the wires.
RJ45 uses 8P8C modular connector, which stands for 8 Position 8 Contact. It is a keyed connector which means that the connector can be inserted only in a single way. RJ45 is used almost exclusively to refer to Ethernet-type computer connectors.

Characteristics of twisted pair cable

1. Requires amplifiers every 5-6 km for analog signals
2. Requires repeaters every 2-3 km for digital signals
3. Attenuation is a strong function of frequency
4. Susceptible to interference and noise

Unshielded Twisted-Pair Connector

Applications

1. Used in telephone lines to provide voice and data channels.
2. The local loop –the line connecting the subscriber to the central telephone office- commonly consists of UTP cables.
3. DSL lines are also UTP cables.
4. LANs such as, 10Base-T and 100Base-T use UTP cables.

Advantages

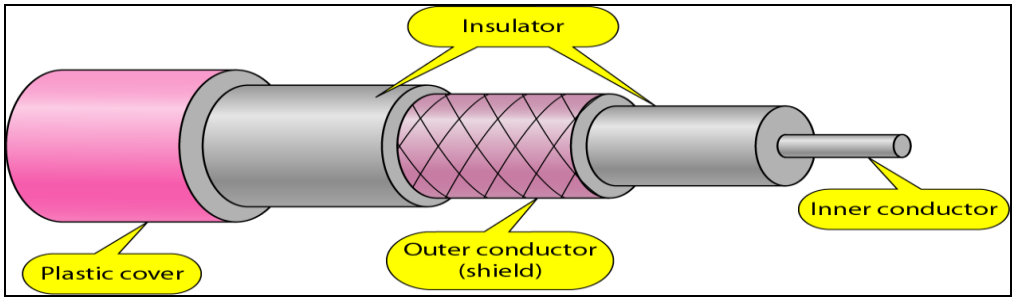
- Inexpensive and readily available
- Flexible and light weight
- Easy to work with and install

Disadvantages

- Susceptibility to interference and noise
- For analog, repeaters needed every 5-6km
- For digital, repeaters needed every 2-3km
- Relatively low bandwidth (3000Hz)

3.4.2 Coaxial Cable

Coaxial cable carries signals of higher frequency ranges than those in twisted-pair cable because the two media are constructed quite differently.
Coaxial cable is an electrical cable, encasing of tubular layers. The whole cable is protected by a plastic cover. This plastic cover, in turn, encloses a tubular insulating sheath. The insulating sheath further encloses a metallic conductor.
The outer metallic wrapping serves both as a shield against noise as well as acts as the second conductor of the circuit. The metallic conductor encircles another insulating sheath. This dielectric sheath encloses the central core conductor of solid wire. The wire is usually copper.



Coaxial Cable

The term coaxial comes from the inner conductor and the outer shield, sharing the same geometric axis.

3.4.2.1 Coaxial Cable Connectors

Coaxial connectors are needed to connect coaxial cable to devices. The most common type of connector used today is the Bayone-Neil-Concelman, in short, BNC connector.
The three popular types of connectors are: the BNC connector, the BNC T connector, and the BNC terminator. The BNC connector is used to connect the end of the cable to a device, such as a TV set.

The BNC T connector is used in Ethernet networks to branch out to a connection to a computer or other device. The BNC terminator is used at the end of the cable to prevent the reflection of the signal.

Coaxial Cable Connector

Applications

1. Coaxial cable was widely used in analog telephone networks, and later with digital telephone networks.
2. Cable TV networks use coaxial cables (RG-59) at the network boundaries. However, coaxial cable has largely been replaced today with fiber-optic cable due to its higher attenuation.
3. Traditional Ethernet LAN
   – 10Base-2, or thin Ethernet, uses RG-58 coax cable with BNC connectors.
   – 10Base-5, or thick Ethernet, uses RG-11 coax cable with specialized connectors.

Advantages

- Higher bandwidth (400 to 600Mhz) can carry up to 10,800 voice conversations
- Can be tapped easily (pros and cons)
- Much less susceptible to interference than twisted pair

Disadvantages

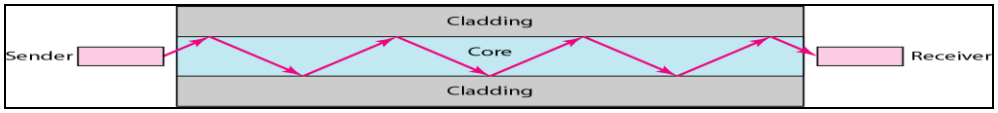
- High attenuation rate makes it expensive over long distance

3.4.3 Fiber optic Cable

Instead of using electric signals to send data, fiber optics cable uses **light**. It works on the principle of total internal reflection.

The cables are made of glass fibers, each thinner than a human hair, that can guide light beams for very long distances. An optical fiber consists of an extremely thin cylinder of glass, called the **core**, surrounded by another layer of glass, known as the **cladding**. The fibers are sometimes made of plastic.

Plastic is easier to install, but cannot carry the light pluses for as long a distance as glass.



Fiber optic Cable

3.4.3.1 Fiber-Optic cable connectors

There are three types of Connectors for fiber optic cable, namely, Subscriber Channel Connector, Straight – Tip Connector and MT – RJ connector.

Fiber Optic Cable Connector

The Subscriber Channel Connector is used for cable TV. It uses a push /pulls locking system. The Straight – Tip Connector is used for connecting cable to networking devices. It uses a bayonet locking system and is more reliable than Subscriber Channel Connector. MT – RJ is a connector that is the same size as RJ45.

Application

1. Often used as backbone networks (like SONET) because its wide bandwidth is cost-effective.
2. Some cable TV companies use a hybrid network: combination of optical-fiber and coaxial cable.
3. LAN such as 100Base-FX network (Fast Ethernet) and 1000Base-X.

Advantages

- High bandwidth capacity (many gigabits per second).
- Longer distances between devices (from 2 to over 60 kilometers).
- Immunity to electromagnetic interferences
- It can also send and receive very high frequencies at one time.
- Less signal attenuation
- Light weight
- Greater immunity to tapping.

Disadvantages

- Installation and maintenance,
- Unidirectional light propagation and cost.

Choice for fiber-optic cable

1. Use fiber-optic cable if you need to transmit data at very high speeds over long distances in very secure media.
2. Do not use fiber-optic cable if you are under a tight budget and do not have the expertise available to properly install it and connect devices to it.

3.5 Comparison between Twisted pair Cable Co axial Cable and Optical fiber

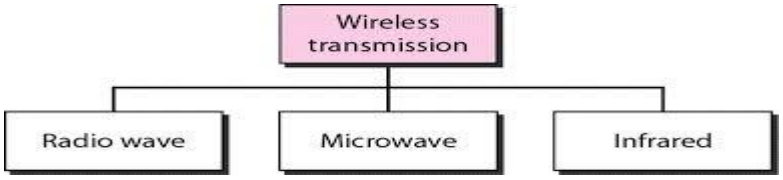
Twisted pair cable	Co-axial cable	Optical fiber
Transmissions of signals take place in the electrical form over the metallic conducting wires.	Transmission of signals take place in the inner conductor of the cable	Signal transmission takes place in an optical form over a glass fiber.
Noise immunity is low. Therefore more distortion	Higher noise immunity than the twisted pair cable due to the presence of shielding conductor	Higher noise immunity as the light rays are unaffected by the electrical noise.
Affected due to external magnetic field	Less affected due to external magnetic field	Not affected by the external magnetic field.
Short circuit between the two conductor is possible	Short circuit between the two conductor is possible	Short circuit is not possible
Cheapest	Moderately expensive	Expensive

Can support low data rates	Moderately high data rate	Very high data rates.
Low bandwidth	Moderately high bandwidth	Very high bandwidth
Easy to installed	Installation is fairly easy	Installation is difficult

3.6 Unguided (Wireless) Medium

Unguided media transport data without using a physical conductor. This type of communication is often referred to as wireless communication. It uses wireless electromagnetic signals to send data. There are three types of Unguided Media

1. Radio waves
2. Micro waves
3. Infrared



Categories of wireless medium

Types of wave propagation

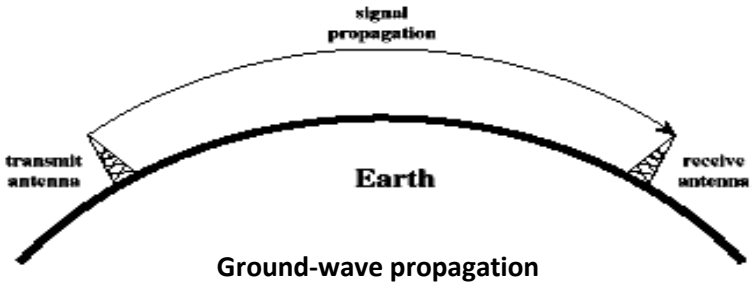
Before understanding the different types of wireless transmission media, let us first understand the ways in which wireless signals travel. These signals can be propagated in three ways:

i. Ground-wave propagation
ii. Sky-wave propagation
iii. Line-of-sight propagation

i. Ground-wave propagation

Characteristics

- Follows contour of the earth
- Can propagate considerable distances
- Frequencies up to 2 MHz
- Example : AM radio

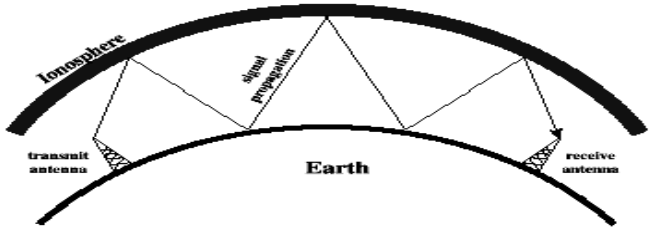


Ground-wave propagation

ii. Sky-wave propagation

Characteristics

- Signal reflected from ionized layer of atmosphere back down to earth
- Signal can travel a number of hops, back and forth between ionosphere and earth‘s surface
- Reflection effect caused by refraction
- Examples
  - Amateur radio
  - CB radio



Sky-wave propagation

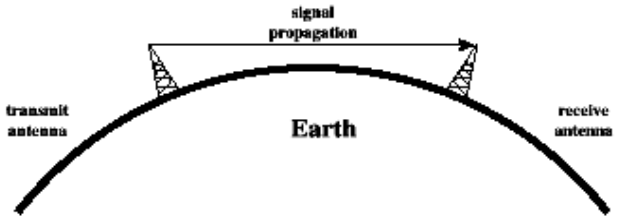
iii. Line-of-sight propagation

Characteristics

i. Transmitting and receiving antennas must be within line of sight

a. **Satellite communication** – signal above 30 MHz not reflected by ionosphere

b. **Ground communication** – antennas within *effective* line of site due to refraction



Line-of-sight propagation

3.6.1 Radio waves

Radio waves are electromagnetic waves ranging in frequencies between 3 KHz and 1GHz. These are Omni-directional; when an antenna transmits radio waves they are propagated in all directions. This means that sending and receiving antenna do not have to be aligned. A sending antenna can send waves that can be received by any receiving antenna. Radio waves propagate in sky mode, can travel long distances. This makes radio waves a good candidate for long-distance broadcasting such as AM radio. Radio waves are of low and medium frequencies can penetrate walls. It is an advantage because; an AM radio can receive signals inside a building.

3.6.2 Microwaves

Electromagnetic waves having frequencies between 1 and 300 GHz are called microwaves.

Microwaves are unidirectional; when an antenna transmits microwaves they can be narrowly focused. This means that the sending and receiving antennas need to be aligned. The unidirectional property has an obvious advantage. A pair of antennas can be aligned without interfering with another pair of aligned antennas. Microwaves propagation is line-of-sight, Since the towers with the mounted antennas needs to be in direct sight of each other, towers that are far apart need to be very tall, the curvature of the earth as well as other blocking obstacles do not allow two short towers to communicate using microwaves, Parabolic dish antenna and horn antenna are used for this means of transmission.

3.6.3 Infrared

Infrared signals with frequencies ranges from 300 GHz to 400 GHz can be used for short range communication. Infrared signals, having high frequencies, cannot penetrate walls. This helps to prevent interference between one system and another. Infrared transmission in one room cannot be affected by the infrared transmission in another room. Transfer digital data is possible with a high speed with a very high frequency. There are number of computer devices which are used to send the data through infrared medium e.g. keyboard mice, PCs and printers.

The choice of transmission media

The choice of the medium is very important since it affects the network cost, maximum operating speed and error rates. A transmission media should be durable, reliable, inexpensive, immune to noise, and easy to install, maintain, and reconfigure.

3.7 Comparison between Guided and Unguided Media

Guided media and unguided media differ from each other in the following ways.

GuidedMedia	Unguided Media
The signal energy is contained and guided within a solid medium	The signal energy propagates in the form of unguided electromagnetic waves.
The examples of wired media are twisted- pair wires, coaxial cable, optical fiber cables.	Microwaves, radio waves and infrared lights are the examples of wireless media.
Used for point to point communication	Used for radio broadcasting in all direction
Wired media lead to discrete network topology	Wireless media leads to continuous network topology
Additional transmission capacity can be procured by adding more wire	It is not possible procure additional capacity.
Installation is costly and time consuming	Installation needs less time and money
Attenuation depends exponentially on the distance.	Attenuation is proportional to square of the distance.

3.8 Network Devices

Local Area Networks are connected to one another using connecting devices. Connecting devices can operate in different layers of the Internet model.
Connecting devices are divided into five different categories based on the layer in which they operate in a network. The five categories contain devices which can be categorized as:

1. Those which operate below the Physical Layer such as a **Passive Hub**.
2. Those which operate at the Physical Layer like a Repeater or an **Active Hub**.
3. Those which operate at the Physical and Data Link Layers such as a **Bridge** or a **two-layer switch**

4. Those which operate at the Physical, Data Link, and Network Layers such as a **router** or **a three - layer switch.**
5. Those which can operate at all five layers such as a **Gateway** as a router.

In this section, we will discuss about network devices that operate in different layers

3.8.1 Hubs

Hubs are commonly used for LAN connectivity. They serve as the central connection points for LANs.

Hubs receive signals from each computer and repeat the signals to all other stations connected to the hub.

Hubs generally have 4 to 24 RJ-45 ports for twisted-pair cabling and one or more uplink ports for connecting the hub to other hubs. Also hubs have indicator lights to indicate the status of the port link status, collisions and so on.

Hub

There are two types of hubs, namely, passive hubs and active hubs. Passive hubs act just as a connector. It connects the wires coming from different branches. In a star-topology Ethernet LAN, a passive hub is just a point where the signals coming from different stations collide. The passive hub is the collision point. This type of a hub is part of the transmission media. Its location in the Internet model is below the physical layer.

Active hubs, also amplify the signal before transmitting it to the other computers. Active hub is actually a Multiport Repeater which operates in the physical layer of the Internet model. It is normally used to create connections between stations in a physical star topology.

3.8.2 Switches

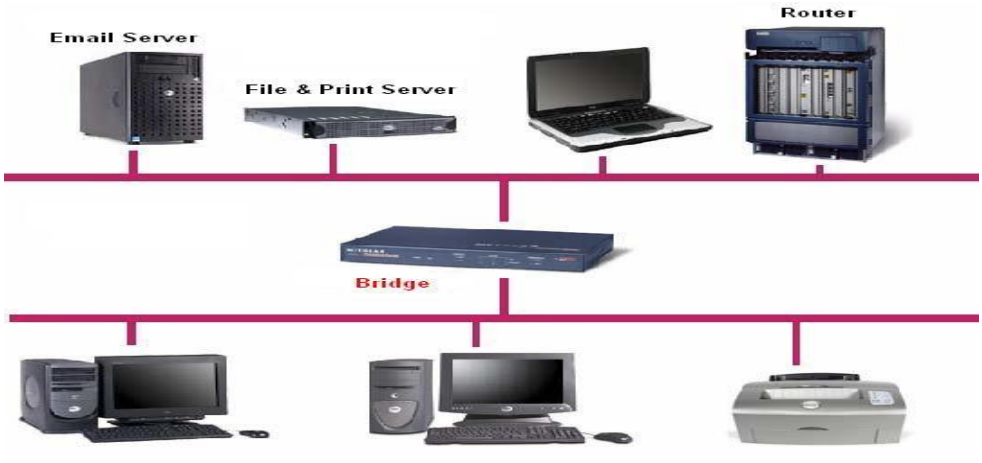
A switch is a network device that selects a path or circuit for sending a signal between source and destination. It determines what adjacent network point, the data should be sent to.

Switch

There are two types of switch, namely, two- layer switch and three- layer switch. The two-layer switch performs at the physical and data link layers. Two-layer switch is a bridge with many ports to connect few LANs together and has better performance. A three-layer switch is used at the network layer as a router. It routes packets based on their logical addresses.
In smaller networks, switch is not required. It is required in large internet works, where there can be many possible ways of transmitting a message from a sender to destination. The purpose of the switch is to select the best possible path so as to manage the bandwidth on a large network.

3.8.3 Bridges

A bridge operates in both the physical and the data link layer. As a physical layer device, it regenerates the signal it receives. As a data link layer device, the bridge can check the physical addresses, i.e. MAC addresses of source and destination contained in the frame. MAC stands for Media Access Control.

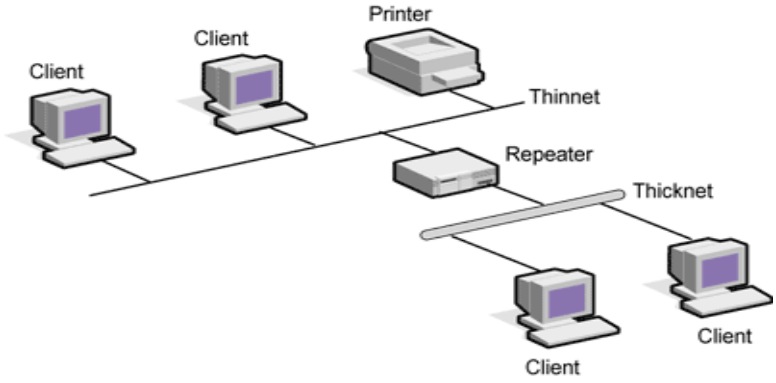


The functionality difference between a bridge and a repeater is that a bridge has filtering capability. A bridge has a table that maps addresses to ports. It can check the destination address of a frame and decide if the frame should be forwarded or dropped. If the frame is to be forwarded, the decision must specify the port.

3.8.4 Repeater

Repeaters are network device that operates only in the Physical Layer. Within a network, signals can travel a fixed distance before attenuation weakens the integrity of the data. A repeater receives a signal just before it becomes too weak or corrupted. It regenerates the original bit pattern and sends the refreshed signal.

A repeater can extend the physical length of a single network. It can overcome the cable length restriction in the network by dividing the cable into segments. Repeaters are installed between segments and act as a two-port node. When it receives a frame from any of the ports, it regenerates and forwards it to the other port.
It is tempting to compare a repeater to an amplifier, but the comparison is inaccurate.



An amplifier cannot discriminate between the intended signal and noise. It amplifies equally everything fed into it.
A repeater does not amplify the signal, but regenerates the signal. When it receives a weakened or corrupted signal, it creates a copy, bit for bit, at the original strength.

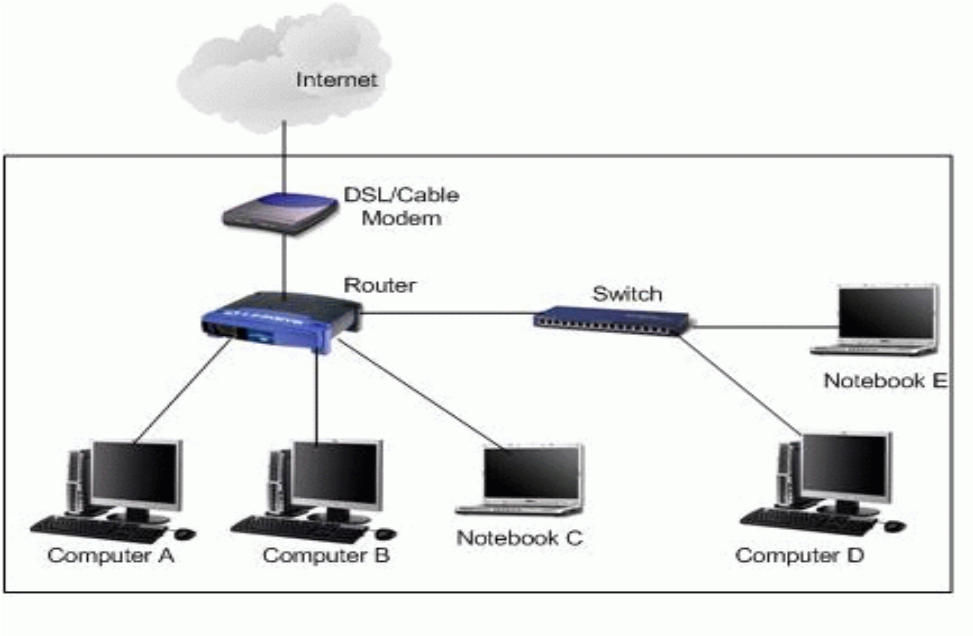
Function of Repeater

The function of a repeater is to regenerate the original signal by creating a copy, bit for bit, at the original strength. A repeater must receive a signal before it becomes too weak or corrupted. Hence, the location of a repeater on a network is vital. It must be placed so that a signal reaches it before any noise changes the meaning of any of its bits. A little noise can alter the precision of a bit's voltage without destroying its identity.
A repeater placed on the line, before the legibility of the signal becomes lost, can still read the signal well enough to determine the intended voltages and replicate them in their original form.

3.8.5 Routers A router is a three-layer device that routes packets based on their logical addresses. A router normally connects LANs and WANs in the Internet and has a routing table that is used for making decisions about the route. The routing tables are normally dynamic and are updated using routing protocols.

Routers are devices that help in determining the best path out of the available paths, for a particular transmission. They consist of a combination of hardware and software. The hardware includes the physical interfaces to the various

networks in the internet work. The two main kinds of software in a router are the operating system and the routing protocol.
Routers use logical and physical addressing to connect two or more logically separate networks.
They accomplish this connection by organizing the large network into logical network segments or sub-networks.
Each of these sub-networks is given a logical address. This allows the networks to be separate but still access each other and exchange data when necessary.



Data is grouped into packets, or blocks of data. Each packet, in addition to having a physical device address, has a logical network address. Since messages are stored in the routers before re-transmission, routers are said to implement a store-and-forward technique.

3.8.6 Gateway

A gateway is normally a computer that operates in all five layers of the Internet or seven layers of OSI model. Gateways handle messages, addresses and protocol conversions necessary to deliver a message between networks.
It takes an application message, reads it, and interprets it. This means that it can be used as a connecting device between two internet works that use different models.
A common use for a gateway is to connect a LAN and a Mainframe computer by changing protocols and transmitting packets between two entirely different networks. For example, a network designed to use the OSI model can be connected to another network using the Internet model. The gateway

connecting the two networks, can take a frame as it arrives from the first network, move it up to the OSI application layer, and remove the message.
It offers the greatest flexibility in internetworking communications. This flexibility is at the cost of higher price, more complex design, implementation, maintenance and operation of a gateway. Gateways can provide security and is used to filter unwanted application-layer messages.
When comparing all the network devices, it is to be noted that a gateway is slower than a router and a router is slower than a bridge, unless the processing capability is raised proportionately.

3.9 Key terms & Concepts

Twisted-Pair (TP) cable consists of two insulated copper wires, twisted together and enclosed in some kind of sheath.

Shielded twisted-pair cable consists of insulated twisted pairs enclosed in a metal foil.

Coaxial cable is a type of cable that uses a center conductor, wrapped by an insulating layer, surrounded by a braided wire mesh and an outer jacket, to carry high-bandwidth signals such as network traffic.

Fiber-optic cable is a cabling technology that uses pulses of light sent along a light conducting fiber at the heart of the cable to transfer information from sender to receiver.

Hub is a central concentration point of a star network

MAC address is the unique address programmed into a NIC that the MAC layer handles.

Network Interface Card (NIC) is a network adapter designed to permit a computer to be attached to one or more types of networking media.

Repeater is a networking device that regenerates electronic signals, so that they can accommodate additional computers on a network segment.

RJ-45 is the eight-wire modular jack for Twisted-Pair networking cables and also for PBX-based telephone systems.

Router is networking device that operates at the Network Layer of the OSI model.

Switch is a special networking device that manages networked connections between any pair of star-wired devices on a network.

3.10 Self-assessment Questions

Short answer type questions

1. What are the advantages and disadvantages of twisted pair cable?
2. What are the characteristics of coaxial cable?
3. What are the advantages and disadvantages of optical fiber cable?
4. What are the characteristics of optical fiber cable?
5. What are the advantages and disadvantages of optical fiber cable?
6. Why is a data link layer switch preferred over a hub?
7. What are the purposes of Bridges?
8. Differentiate between a hub and switch.
9. Differentiate between router & bridge.
10. Which device is needed to connect two LANs with different network IDs

Long answer type questions

1. Describe the construction and components of fiber optic cable. Write its features advantages and disadvantages.
2. Differentiate the features of twisted pair, coaxial cable and fiber optic cables.
3. Discuss the features of wireless transmission media.
4. Differentiate between the wired and wireless transmission media.
5. Discuss the functions of different network devices in functioning of computer networks.

3.11 References and Suggested Readings

1. Behrouz A. **Forouzan**, "*Introduction to Data Communications and Networking***",** McGraw-Hill Education (India), New Delhi.
2. Andrew S. **Tanenbaum**, "*Computer Networks*", PHI Learning Pvt. Ltd
3. James F. **Kurose,** Keith W. **Ross**, "*Computer Networking: A Top-Down Approach Featuring the Internet*", Pearson Education Inc., New Delhi.
4. Wayne **Tomasi,** "*Introduction to Data Communications and Networking*", Pearson Education Inc., New Delhi.
5. L. L. **Peterson &** B. S. **Davie**," *Computer Networks*", Elsevier Inc,