SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

School of Computing

Department of Computer Science and Engineering

UNIT - I

Data Communication and
Computer Networks-SBS1302

UNIT I PROTOCOLS & MEDIA

Introduction to data communication – Network protocols & standards – Line configuration – Topology – Transmission mode – Classification of Network OSI Model- Layers of OSI model.

1. Introduction to Data Communications

A **computer network**, often simply referred to as a network, is a collection of computers and devices interconnected by communications channels that facilitate communications and allows sharing of resources and information among interconnected devices. **Computer networking** is the engineering discipline concerned with the computer networks. Computer networking is sometimes considered a sub-discipline of electrical engineering, telecommunications, computer science, information technology and/or computer engineering since it relies heavily upon the theoretical and practical application of these scientific and engineering disciplines

Data Communications

The transmission of data to and from computers and components of computer systems. The subset of business telecommunications that addresses the processes, equipment, facilities, and services used to transport data from devices at one location to devices at other locations.

Essential Features of Communication

Message

Types of data communication messages include:

- file - group of related items
- request - from sender to receiver for some action to beperformed response - from receiver back tosender
- status - status of the system (e.g. system going down in 5 minutes) control - sent between system components (e.g. printer out ofpaper) correspondence - sent from user touser
- Sender-Originator of the message, either a person or a machine. Receiver-Destination of the message.
- Medium-Where the message physically travels to get from sender to receiver. Understandability
- A message must be understood before communications has taken place.
- Error Detection-How to determine if the message was changed during transmission.

Essential Features of Networks

- **Network** – At least one sender and one receiver connected by a communication medium.
- **Session** – The exchange of messages between two users over a network.
- **Node** - Device that is connected to a network
- **Link** - The circuit between two adjacent nodes, with no intervening nodes. **Path** - One or more links that allows a message to travel from sender to receiver **Circuit** - Either the medium connecting two devices or apath
- **Virtual Circuit** – A temporary communications path created between two nodes in a switched communication network.
- **Packetizing** – Dividing a message into packets prior to transmitting the message over a communication medium.

- **Packet Switching** - The transmission of a message by dividing the message into fixed-length packets and then routing the packets to the recipient. Packets may be sent over different paths and arrive out of order.
- **Routing** - How the path from sender to receiver is determined
- **Store-and-Forward** - The messages are stored at intermediate nodes and then forwarded to the next node.
- **Network Topology** - The physical form the network takes
- **Network Architecture** - The way in which media, hardware, and software are integrated to form a network.

When we communicate, we are sharing information. This sharing can be local or remote. between individuals, local communication usually occurs face to face, while remote communication takes place over distance. The term Telecommunication, which includes Telephony, Telegraphy, and television, means communication at a distance.

The data refers to facts, concepts and instruction presented in whatever form is agreed upon by the parties creating and using the data. In the context of computer information system, data represented by binary information units produced and consumed in the form of 0s and 1s.

Data Communications is the transfer of data or information between a source and a receiver. The source transmits the data and the receiver receives it. The actual generation of the information is not part of Data Communications nor is the resulting action of the information at the receiver. Data Communication is interested in the transfer of data, the method of transfer and the preservation of the data during the transfer process.

The purpose of Data Communications is to provide the rules and regulations that allow computers with different disk operating systems, languages, cabling and locations to share resources. The rules and regulations are called protocols and standards in Data Communications.

For data communication to occur, the communicating devices must be part of a communication system made up of a combination of hardware and software. The effectiveness of a data communication system depends on the three fundamental characteristics:

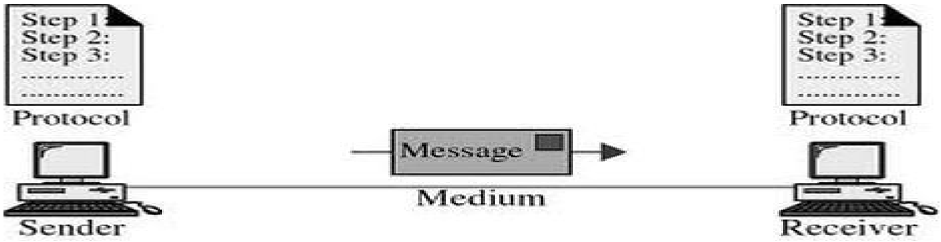
1. **Delivery**: The System must deliver data to the correct destination. Data must be received bythe intended device or user and only by that device or user
2. **Accuracy**: The system must deliver data accurately. Data that have been altered in transmission and left uncorrected arerustles
3. **Timeliness**: The system must deliver data in a timely manner. Data delivered late are useless. In the case of video, audio, and voice data, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. this kind of delivery id called real- timetransmission.

Components

Basic Components of a Communication System

The following are the basic requirements for working of a communication system.

1. The sender (source) who creates the message to betransmitted
2. A medium that carries themessage



3. The receiver (sink) who receives themessage

Fig 1 Data Communication system components

1. **Message:** A message in its most general meaning is an object of communication. It is a vessel which provides information. Yet, it can also be this information. Therefore, its meaning is dependent upon the context in which it is used; the term may apply to both the information and itsform.

2. **Sender**: The sender will have some kind of meaning she wishes to convey to the receiver. It might not be conscious knowledge, it might be a sub-conscious wish for communication. What is desired to be communicated would be some kind of idea, perception, feeling, or datum. It will be a part of her reality that she wishes to send to somebodyelse.

3. **Receiver**: These messages are delivered to another party. No doubt, you have in mind a desired action or reaction you hope your message prompts from the opposite party. Keep in mind, the other party also enters into the communication process with ideas and feelings that will undoubtedly influence their understanding of your message and their response. To be a successful communicator, you should consider these before delivering your message, then actingappropriately.

4. **Medium:** Medium is a means used to exchange / transmit the message. The sender must choose an appropriate medium for transmitting the message else the message might not be conveyed to the desired recipients. The choice of appropriate medium of communication is essential for making the message effective and correctly interpreted by the recipient. This choice of communication medium varies depending upon the features of communication. For instance - Written medium is chosen when a message has to be conveyed to a small group of people, while an oral medium is chosen when spontaneous feedback is required from the recipient as misunderstandings are cleared then andthere.

5. **Protocol**: A protocol is a formal description of digital message formats and the rules for exchanging those messages in or between computing systems and in telecommunications. Protocols may include signaling, authentication and error detection and correction syntax, semantics, and synchronization of communication and may be implemented in hardware or software, orboth.

6. **Feedback**: Feedback is the main component of communication process as it permits the sender to analyze the efficacy of the message. It helps the sender in confirming the correct interpretation of message by the decoder. Feedback may be verbal (through words) or non-verbal (in form of smiles, sighs, etc.). It may take written form also in form of memos, reports, etc.

Networks

Networking is the practice of linking two or more computing devices together for the purpose of sharing data. Networks are built with a mix of computer hardware and computer software.

Distributed Processing

Distributed computing is a field of computer science that studies distributed systems. A distributed system consists of multiple autonomous computers that communicate through a computer network. The computers interact with each other in order to achieve a common goal. A computer program that runs in a distributed system is called a distributed program, and distributed programming is the process of writing such programs.

Distributed computing also refers to the use of distributed systems to solve computational problems. In distributed computing, a problem is divided into many tasks, each of which is solved by one or more computers.Distributed programming typically falls into one of several basic architectures or categories: client–server, 3-tier architecture, n-tier architecture, distributed objects, loose coupling,or tightcoupling.

- **Client–server**: Smart client code contacts the server for data then formats and displays it to the user. Input at the client is committed back to the server when it represents a permanentchange.
- **3-tier architecture:** Three tier systems move the client intelligence to a middle tier so that stateless clients can be used. This simplifies application deployment. Most web applications are3-Tier.
- ***n*-tier architecture:** n-tier refers typically to web applications which further forward their requests to other enterprise services. This type of application is the one most responsible for the success of applicationservers.
- **Tightly coupled (clustered):** refers typically to a cluster of machines that closely work together, running a shared process in parallel. The task is subdivided in parts that are made individually by each one and then put back together to make the finalresult.
- **Peer-to-peer:** an architecture where there is no special machine or machines that provide a service or manage the network resources. Instead all responsibilities are uniformly divided among all machines, known as peers. Peers can serve both as clients andservers.

- **Space based:** Refers to an infrastructure that creates the illusion (virtualization) of one single address-space. Data are transparentlyreplicated. According to application needs. Decoupling in time, space and reference is achieved.

2. Protocols and Standards

Protocols:

In computer networks, communication occurs between entries in different systems. An entity is anything capable of sending or receiving information. But two entities cannot communicate each other as sending or receiving. For communication occurs the entities must agree on aprotocol.

A protocol is a set of rules that govern data communication. A protocol defines what is communicated how it is communicated, and when it is communicated. The key elements of a protocol are syntax, semantics and timing.

Syntax:

Syntax refers to the structure or format of the data, means to the order how it is presented.

Semantics:

Semantics refers to the meaning of each section of bits. How is a particular pattern to be interpreted, and when action is to be taken based on theinterpretation.

Timing:

Timing refers to two characteristics. They are,

1. When data should besent
2. When data to bereceived.

Standards:

A standard provides a model for development of a product, which is going to develop. Standards are essential to create and maintain a product.

Standards Organization

1. Standards creationcommittees:

1. International Standards Organization (ISO)

2. International Telecommunications Union – Telecommunications Standards Section (ITU-T formallyCCITT)
3. The American National Standards Institute(ANSI)
4. The Institute of Electrical and Electronics Engineers(IEEE)
5. The Electronic Industries Association(EIA)
6. Telcordia

2. Forums:

1. Frame RelayForum
2. ATM Forum & ATMconsortium
3. Internet Society (ISOC) & Internet Engineering Task Force(IETF)

3. RegularityAgencies:

StandardscreationCommunities

IEEE (Institute of Electrical and Electronics Engineers) IEEE's Constitution defines the purposes of the organization as "scientific and educational, directed toward the advancement of the theory and practice of Electrical, Electronics, Communications and Computer Engineering, as well as Computer Science, the allied branches of engineering and the related arts and sciences." The IEEE is incorporated under the Not-for-Profit Corporation Law of the state of New York, United States. It was formed in 1963 by the merger of the Institute of Radio Engineers (IRE, founded 1912) and the American Institute of Electrical Engineers (AIEE, founded 1884). It has more than 400,000 members in more than 160 countries, 45% outside the United States.In pursuing these goals, the IEEE serves as a major publisher of scientific journals and a conference organizer. It is also a leading developer of industrial standards (having developed over 900 active industry standards) in a broad range of disciplines, including electric power and energy, biomedical technology and health care, information technology, information assurance, telecommunications, consumer electronics, transportation, aerospace, and nanotechnology. IEEE develops and participates in educational activities such as accreditation of electrical engineering programs in institutes of higherlearning.

IEEE is one of the leading standards-making organizations in the world. IEEE performs its standards making and maintaining functions through the IEEE Standards Association

(IEEE-SA). IEEE standards affect a wide range of industries including: power and energy, biomedical and health care, Information Technology (IT), telecommunications, transportation, nanotechnology, information assurance, and many more. In 2005, IEEE had close to 900 active standards, with 500 standards under development. One of the more notable IEEE standards is the IEEE 802 LAN/MAN group of standards which includes the IEEE 802.3 Ethernet standard and the IEEE 802.11 WirelessNetworking

ANSI(AmericanNational Standards Institute)standard

Though ANSI itself does not develop standards, the Institute oversees the development and use of standards by accrediting the procedures of standards developingorganizations.

ANSI accreditation signifies that the procedures used by standards developing organizations meet the Institute's requirements for openness, balance, consensus, and due process.
ANSI was originally formed in 1918, when five engineering societies and three government agencies founded the American Engineering Standards Committee (AESC). In 1928, the AESC became the American Standards Association (ASA). In 1966, the ASA was reorganized and became the United States of America Standards Institute (USASI). The present name was adopted in 1969.Prior to 1918, these five engineering societies:

- American Institute of Electrical Engineers (AIEE, nowIEEE)
- American Society of Mechanical Engineers(ASME)
- American Society of Civil Engineers(ASCE)
- American Institute of Mining Engineers (AIME, nowAmerican Institute of Mining, Metallurgical, and PetroleumEngineers)
- American Society for Testing and Materials (nowASTM International)

ANSI also designates specific standards as American National Standards, or ANS, when the Institute determines that the standards were developed in an environment that is equitable, accessible and responsive to the requirements of various stakeholders.

The American National Standards process involves:

- Consensus by a group that is open to representatives from all interestedparties
- Broad-based public review and comment on draft standards
- consideration of and response tocomments
- Incorporation of submitted changes that meet the same consensusrequirements into a draftstandard
- Availability of an appeal by any participant alleging that these principles werenot respected during the standards-developmentprocess.

ITU (International Telecommunications Union - formerly CCITT)

The International Telecommunication Union is the specialized agency of the United Nations which is responsible for information and communication technologies. ITU coordinates the shared global use of the radio spectrum, promotes international cooperation in assigning satellite orbits, works to improve telecommunication infrastructure in the developing world and establishes worldwide standards. ITU coordinates the shared global use of the radio spectrum, promotes international cooperation in assigning satellite orbits, works to improve telecommunication infrastructure in the developing world and establishes worldwide standards.ITU also organizes worldwide and regional exhibitions and forums, such as ITU TELECOM WORLD, bringing together representatives of government and the telecommunications and ICT industry to exchange ideas, knowledge and technology.The ITU is active in areas including broadband Internet, latest-generation wireless technologies, aeronautical andmaritimenavigation,radioastronomy,satellite-basedmeteorology,convergenceinfixed-mobile phone, Internet access, data, voice, TV broadcasting, and next-generation networks.

ISO (International Organization for Standards)

The International Organization for Standardization widely known as ISO, is an international standard-setting body composed of representatives from various national standards organizations. Founded on February 23, 1947, the organization promulgates worldwide proprietary industrial and commercial standards. It has its headquarters in Geneva, Switzerland. While ISO defines itself as a non-governmental organization, its ability to set standards that often become law, either through treaties or national standards, makes it more powerful than most non-governmental organizations. In practice, ISO acts as a consortium with strong links to governments ISO, is an international standard-setting body composed of representatives from various national standards organizations the organization promulgates worldwide proprietary industrial and commercial standards.ISO's main products are the International Standards. ISO also publishes Technical Reports, Technical Specifications, Publicly Available Specifications,Technical Corrigenda, andGuides.

EIA(ElectronicIndustriesAssociation)

The Electronic Industries Alliance (EIA, until 1997 Electronic Industries Association) was a standards and trade organization composed as an alliance of trade associations for electronics manufacturers in the United States. They developed standards to ensure the equipment of different manufacturers was compatible and interchangable.In 1924 the

Associated Radio Manufacturers alliance was formed, which was renamed to Radio Manufacturers Association (RMA) the same year. Upcoming new electronic technologies brought new members and further name changes: Radio Television Manufacturers Association (RTMA) (1950), Radio Electronics Television Manufacturers (RETMA) (1953) and Electronics Industries Association (EIA) (1957). The last renaming took place in 1997, when EIA became Electronics Industries Alliance (EIA), reflecting the change away from a pure manufacturers associationA standard defining serial communication between computers and modems e. g. was originally drafted by the radio sector as RS-232. Later it was taken over by the EIA as EIA-232. Later this standard was managed by the TIA and the name was changed to the current TIA-232. Because the EIA was accredited by ANSI to help develop standards in its areas, the standards are often described as e. g. ANSI TIA-232(or formerly asANSI EIA/TIA-232').

ETSI(EuropeanTelecommunicationsStandards Institute)

The European Telecommunications Standards Institute (ETSI) is an independent, non-profit, standardization organization in the telecommunications industry (equipment makers and network operators) in Europe, with worldwide projection. ETSI has been successful in standardizing the Low Power Radio, Short Range Device, GSM cell phonesystemand theTETRAprofessional mobileradio system.Significant ETSI standardization bodies include TISPAN (for fixed networks and Internetmachine-to-machine communications). ETSI inspired the creation of, and is a partner in 3GPP.

ETSI was created by CEPT in 1988 and is officially recognized by the European Commission and the EFTA secretariat. Based in Sophia Antipolis (France), ETSI is officially responsible for standardization of Information and Communication Technologies (ICT) within Europe. These technologies include telecommunications, broadcasting and related areas such as intelligent transportation and medical electronics. ETSI has 740 members from 62 countries/provinces inside and outside Europe, including manufacturers, network operators, administrations, service providers, research bodies and users — in fact, all the key players in the ICT arena. convergence) and M2M (for ETSI has been successful in standardizing the Low Power Radio, Short Range Device, GSMTETRA professional mobile radio system.ETSI was created by CEPT in 1988 and is officially recognized by the European Commission and the EFTASophia Antipolis (France), ETSI is officially responsible for standardization of Information and Communication Technologies (ICT) within Europe. These technologies include telecommunications, broadcasting and related areas such as intelligent transportationand medical electronics.

W3C - World Wide Web Consortium

The World Wide Web Consortium (W3C) is the main international standards organizationWorld Wide Web (abbreviated WWW or W3).Founded and headed by Tim Berners-Lee,the consortium is made up of member organizations which maintain full-time staff for the purpose of working together in the development of standards for the World Wide Web. As of 18 February 2011, the World Wide Web Consortium (W3C) has 322 members.

W3C also engages in education and outreach, develops software and serves as an open forum for discussion about the Web.

W3C also engages in education and outreach, develops software and serves as an open forum for discussion about the Web.W3C was created to ensure compatibility and agreement among industry members in the adoption of new standards. Prior to its creation, incompatible versions of HTML were offered by different vendors, increasing the potential for inconsistency between web pages. The consortium was created to get all those vendors to agree on a set of core principles and components which would be supported by everyone.

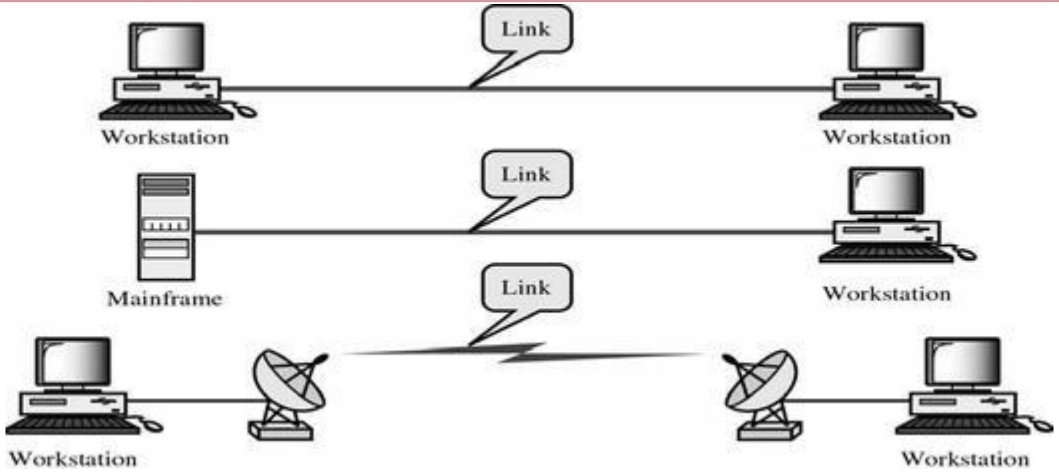
3. Line Configuration

Line configuration refers to the way two or more communication devices attached to a link. Line configuration is also referred to as connection. A Link is the physical communication pathway that transfers data from one device to another. For communication to occur, two devices must be connected in same way to the same link at the same time.
There are two possible line configurations.

1. Point-to-Point.
2. Multipoint.

Point-to-Point

A **Point to Point Line Configuration** Provide dedicated link between two devices use actual length of wire or cable to connect the two end including microwave & satellite link. Infrared remote control &tvs remote control.
The entire capacity of the channel is reserved for transmission between those two devices. Most point-to-point line configurations use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible.
Point to point network topology is considered to be one of the easiest and most conventional network topologies. It is also the simplest to establish and understand. To visualize, one can consider point to point network topology as two phones connected end to



end for a two way communication

Fig 2 Point to Point Communication

Multipoint Configuration

Multipoint Configuration also known as **Multidrop line configuration:** one or more than two specific devices share a single link capacity of the channel is shared.

More than two devices share the Link that is the capacity of the channel is shared now. With shared capacity, there can be two possibilities in a Multipoint Line Config:

- **Spatial Sharing**: If several devices can share the link simultaneously, its called Spatially shared lineconfiguration

- **Temporal (Time) Sharing**: If users must take turns using the link , then its called Temporally shared or Time Shared LineConfiguration.

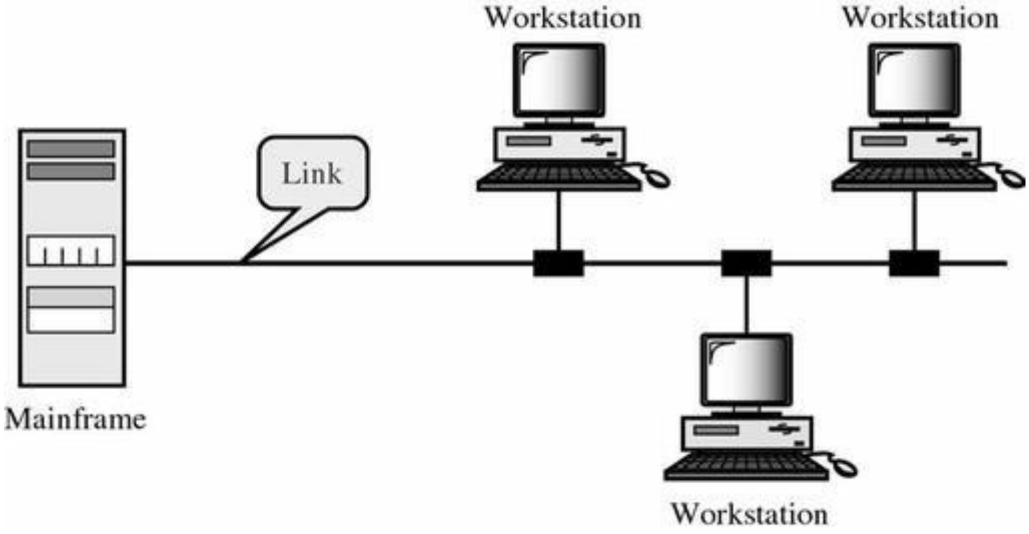


Fig 3 Multi point Configuration

4. Topology

The term "Topology" refers to the way in which the end points or stations/computer systems, attached to the networks, are interconnected. We have seen that a topology is essentially a stable geometric arrangement of computers in a network. If you want to select a topology for doing networking. You have attention to the followingpoints.

- Application S/W andprotocols.
- Types of data communicatingdevices.
- Geographic scope of thenetwork.
- Cost.
- Reliability.

Depending on the requirement there are different Topologies to construct a network.

1. Meshtopology.
2. Startopology.
3. Tree (Hierarchical)topology.
4. Bustopology.
5. Ring topology.
6. Cellulartopology.

Ring and mesh topologies are felt convenient for peer topeer transmission.Star and tree are more convenient for clientserver.Bus topology is equally convenient for either ofthem.

Mesh Topology

The value of fully meshed networks is proportional to the exponent of the number of subscribers, assuming that communicating groups of any two endpoints, up to and including all the endpoints, is approximated by Reed's Law.

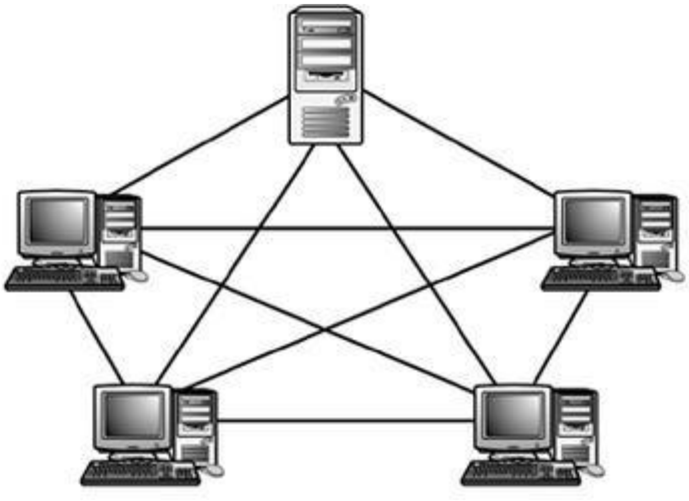


Fig 4 Mesh Topology

Here every device has a dedicated point to point link to every other device. A fully connected mesh can have n(n-1)/2 physical channels to link n devices. It must have n-1 IOports.

Advantages:

1. They use dedicated links so each link can only carry its own data load. So traffic problem can be avoided.
2. It is robust. If any one link get damaged it cannot affectothers
3. It gives privacy andsecurity
4. Fault identification and fault isolation areeasy.

Disadvantages:

1. The amount of cabling and the number IO ports required are very large. Since every device is connected to each other devices through dedicatedlinks.
2. The sheer bulk of wiring is larger then the availablespace

3. Hardware required to connect each device is highlyexpensive.

Example:

A mesh network has 8 devices. Calculate total number of cable links and IO ports needed.

Solution:

Number of devices = 8 Number of links = n (n-1)/2

= 8(8-1)/2

= 28

Number of port/device = n-1

= 8-1 = 7

Star Topology

In a star topology, cables run from every computer to a centrally located device called a HUB. Star topology networks require a central point of connection between media segment. These central points are referred to as Hubs.Hubs are special repeaters that overcome the electromechanical limitations of a media. Each computer on a star network communicates with a central hub that resends the message either to all the computers. (In a broadcast network) or only the destination computer. (In a switched network).Ethernet 10 base T is a popular network based on the star topology.

Here each device has a dedicated link to the central „hub". There is no direct traffic between devices. The transmission are occurred only through the central controller namely hub.

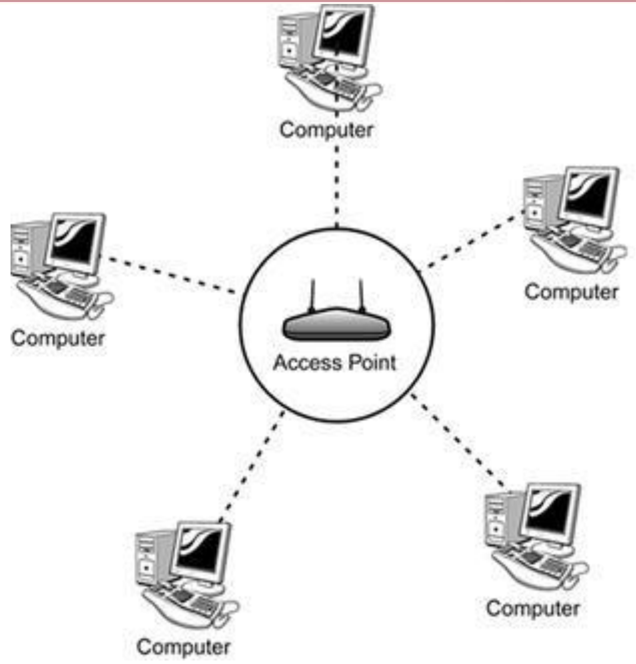


Fig 5 Star Topology

Advantages:

1. Less expensive then mesh since each device is connected only to thehub.
2. Installation and configuration areeasy.
3. Less cabling is need thenmesh.
4. Robustness.
5. Easy to fault identification &isolation.

Disadvantages:

1. Even it requires less cabling then mesh when compared with other topologies it stilllarge.

Tree (Hierarchical) topology

It is similar to the star network, but the nodes are connected to the secondary hub that in turn is connected to the central hub.The central hub is the active hub.The active hub contains the repeater, which regenerates the bits pattern it receives before sending them out.The secondary hub can be either active or passive.

A passive hub provides a simple physical connection between the attached devices.

Advantages:

1. Can connect more thanstar.
2. The distance can beincreased.
3. Can isolate and prioritize communication between different computers.

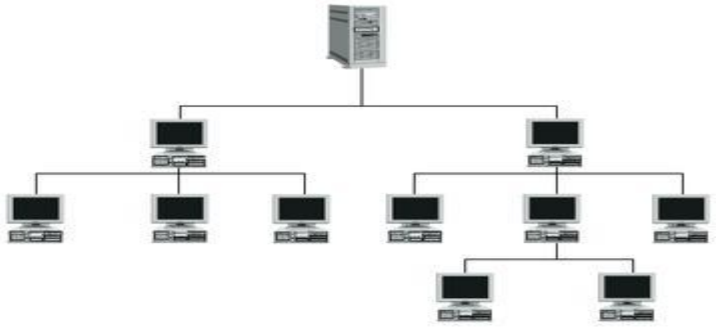


Fig 6 Tree Topology

Bus topology

A bus topology connects computers along a single or more cable to connect linearly. A network that uses a bus topology is referred to as a "bus network" which was the original form of Ethernet networks. Ethernet 10Base2 (also known as thinnet) is used for bus topology.

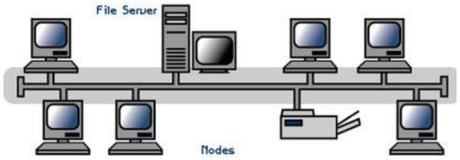


Fig 7 Bus Topology

Advantages:

1. Ease ofinstallation.
2. Lesscabling.

Disadvantages:

1. Difficult reconfiguration and faultisolation.
2. Difficult to add newdevices.
3. Signal reflection at top can degradation inquality
4. If any fault in backbone can stops alltransmission.

Ring topology

In ring topology, each device has a dedicated point-to-point line configuration only with two devices on either side of it.A signal is passed along the ring in one direction, from device to device until it reaches its destination.Each device in the ring has a repeater. When the devices receive the signal intended for the other node, it just regenerates the bits and passes them along.Ring network passes a token.A token is a short message with the electronic address of the receiver.Each network interface card is given a unique electronic address, which is used to identify the computer on the network.

Advantages:

1. Easy toinstall.
2. Easy toreconfigure.
3. Fault identification iseasy.

Disadvantages:

1. Unidirectionaltraffic.
2. Break in a single ring can break entire network.

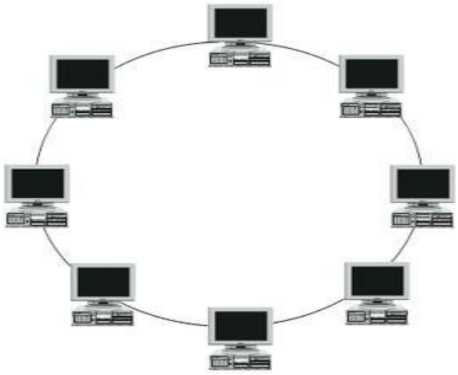


Fig 8 Ring Topology

Cellular topology

The cellular topology is applicable only in case of wireless media that does not require cable connection. In wireless media, each point transmits in a certain geographical area called a cell. Each cell represents a portion of the total network area. Devices that are in the cell communicate through a central hub. Hubs in different cells are interconnected. They route data across the network and provide a complete network infrastructure. The data is transmitted in the cellular digital packet data (CDPD) format.

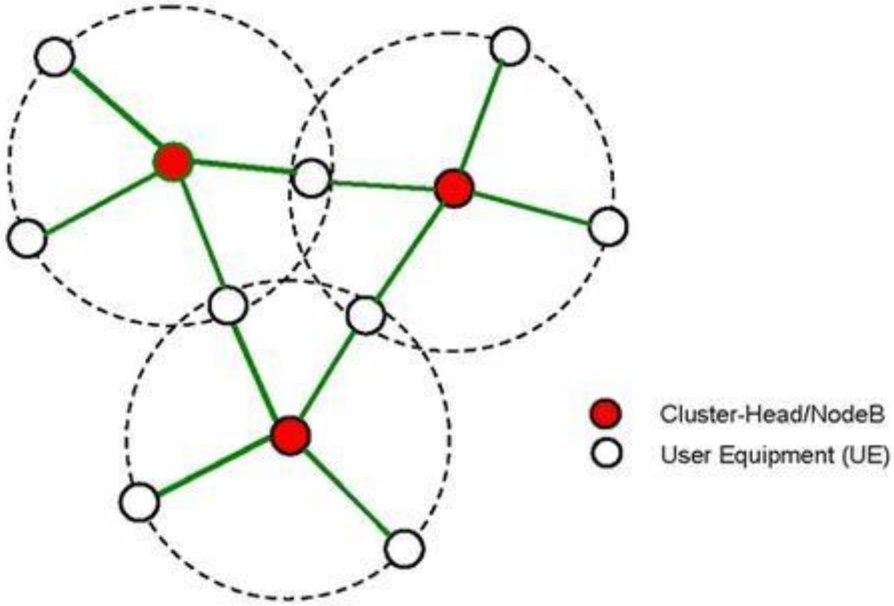


Fig 9 Cellular Topology

5. Transmission Mode

A given transmission on a communications channel between two machines can occur in several different ways. The transmission is characterized by:

- The direction of theexchanges
- The transmission mode: the number of bits sentsimultaneously
- Synchronization between the transmitter andreceiver

Types of Transmission mode

- Simplex
- HalfDuplex
- FullDuplex

Simplex

A simplex connection is a connection in which the data flows in only one direction,from the transmitter to the receiver. This type of connection is useful if the data do not need to flow in both directions (for example, from your computer to the printer or from the mouse to yourcomputer...).

Half Duplex

A half-duplex connection (sometimes called an *alternating connection* or *semi-duplex*) is a connection in which the data flows in one direction or the other, but not both at the same time. With this type of connection, each end of the connection transmits in turn.
This type of connection makes it possible to have bidirectional communications using the full capacity of the line.

Full Duplex

A full-duplex connection is a connection in which the data flow in both directions simultaneously. Each end of the line can thus transmit and receive at the same time, which means that the bandwidth is divided in two for each direction of data transmission if the same transmission medium is used for both directions of transmission.

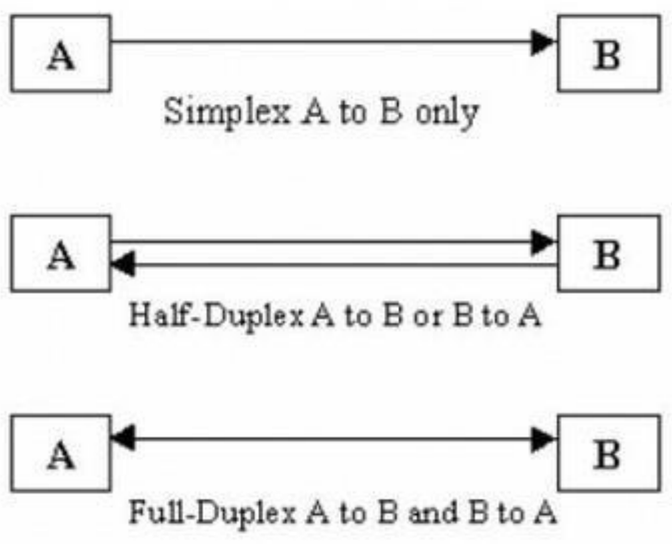


Fig 10 Types of Transmission Mode

Networks

Networking is the practice of linking two or more computing devices together for the purpose of sharing data. Networks are built with a mix of computer hardware and computer software.

Distributed Processing

Distributed computing is a field of computer science that studies distributed systems.
A distributed system consists of multiple autonomous computers that communicate through a computer network. The computers interact with each other in order to achieve a common

goal. A computer program that runs in a distributed system is called
a distributed program, and distributed programming is the process of writing such programs.

Distributed computing also refers to the use of distributed systems to solve computational problems. In distributed computing, a problem is divided into many tasks, each of which is solved by one or more computers.

Distributed programming typically falls into one of several basic architectures or categories: client–server, 3-tier architecture, n-tier architecture, distributed objects, loose coupling, or tight coupling.

- **Client–server:** Smart client code contacts the server for data then formats and displays it to the user. Input at the client is committed back to the server when it represents a permanent change.

- **3-tier architecture:** Three tier systems move the client intelligence to a middle tier so that stateless clients can be used. This simplifies application deployment. Most web applicationsare 3-Tier.
- ***n*-tier architecture:** *n*-tier refers typically to web applications which further forward their requests to other enterpriseservices. This type of application is the one most responsible for the success of applicationservers.
- **Tightly coupled (clustered):** refers typically to a cluster of machines that closely work together, running a shared processin parallel. The task is subdivided in parts that are made individually by each one and then put back together to make the final result.
- **Peer-to-peer:** an architecture where there is no special machine or machines that provide a service or manage the network resources. Instead all responsibilities are uniformly divided among all machines, known as peers. Peers can serve both as clients andservers.
- **Space based:** refers to an infrastructure that creates the illusion (virtualization) of one single address-space. Data are transparently replicated according to application needs. Decoupling in time, space and reference isachieved.

6. Categories of Network

One way to categorize the different types of computer network designs is by their scope or scale. For historical reasons, the networking industry refers to nearly every type of design as some kind of area network. Common examples of area network types are:

- LAN - Local AreaNetwork
- WLAN - Wireless Local AreaNetwork
- WAN - Wide AreaNetwork
- MAN - Metropolitan Area Network

Local Area Network

A LAN connects network devices over a relatively short distance. A networked office building, school, or home usually contains a single LAN, though sometimes one building will contain a few small LANs (perhaps one per room), and occasionally a LAN will span a group of nearby buildings. In TCP/IP networking, a LAN is often but not always implemented as a single IP subnet. In addition to operating in a limited space, LANs are also typically owned, controlled, and managed by a single person or organization. They also tend to use certain connectivity technologies, primarily Ethernet and Token Ring.

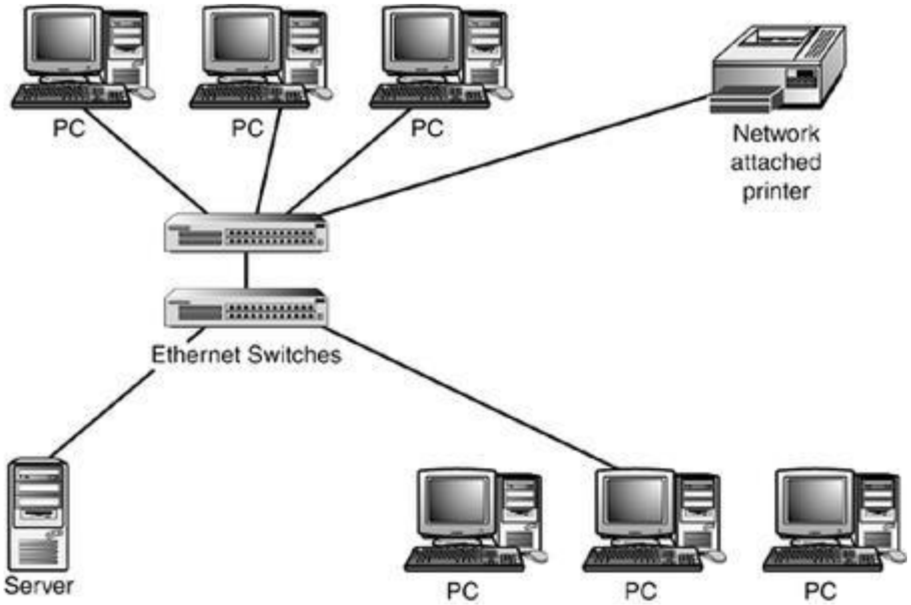


Fig 11 Local Area Network

Wireless Local Area Network

As the term implies, a WAN spans a large physical distance. The Internet is the largest WAN, spanning the Earth. A WAN is a geographically-dispersed collection of LANs. A network device called a router connects LANs to a WAN. In IP networking, the router maintains both a LAN address and a WAN address.

A WAN differs from a LAN in several important ways. Most WANs (like the Internet) are not owned by any one organization but rather exist under collective or distributed ownership and management. WANs tend to use technology like ATM, Frame Relay and X.25 for connectivity over the longer distances.

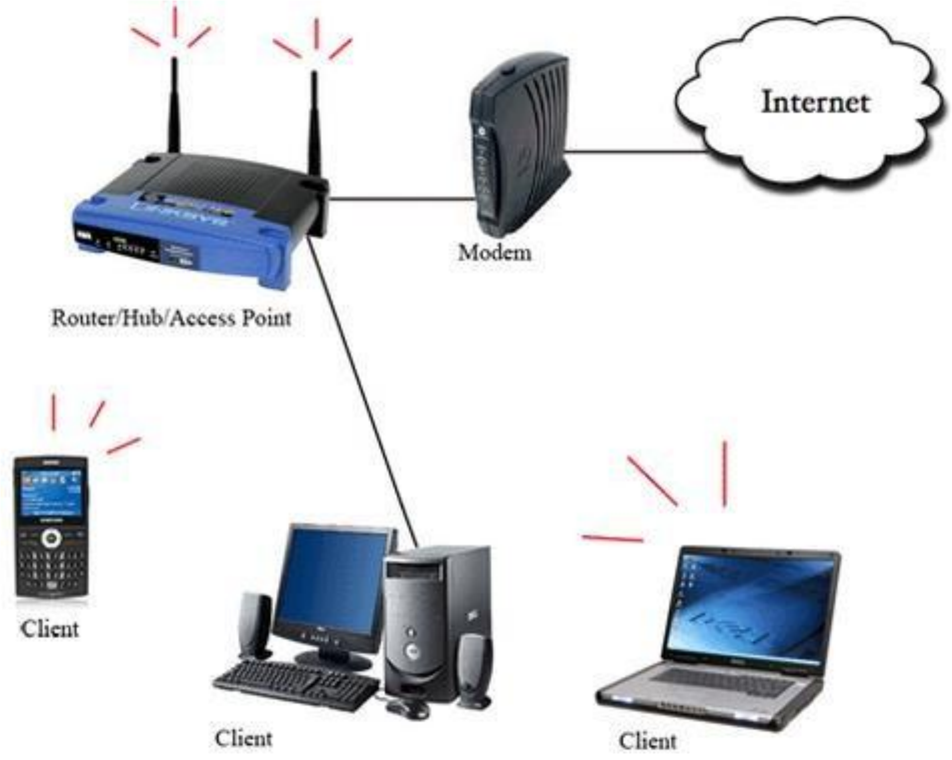


Fig 12 Wireless Local Area Network

Wide Area Network

A WAN is a network that spans more than one geographical location often connecting separated LANs. WANs are slower than LANs and often require additional and costly hardware such as routers, dedicated leased lines, and complicated implementation procedures.

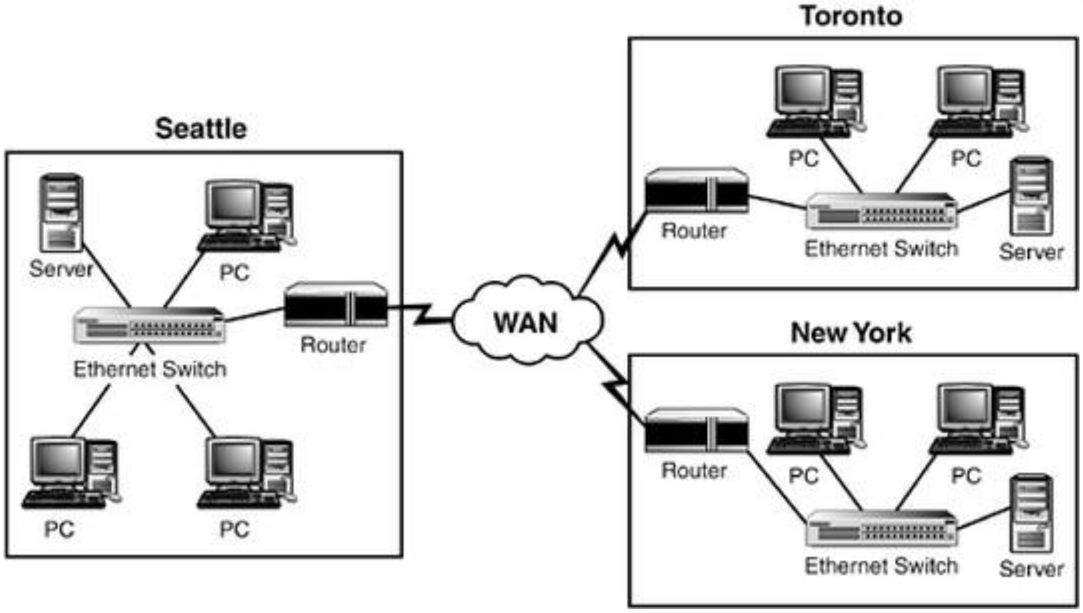


Fig 13 Wide Area Network

Metropolitan Area Network

A network spanning a physical area larger than a LAN but smaller than a WAN, such asa city. A MAN is typically owned an operated by a single entity such as a government body or largecorporation.

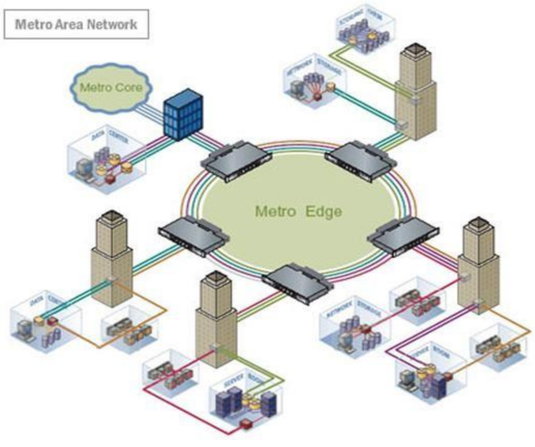


Fig 14 Metropolitan Area Network

7. ISO / OSI Model:

ISO refers International Standards Organization was established in 1947, it is a multinational body dedicated to worldwide agreement on international standards.

OSI refers to Open System Interconnection that covers all aspects of network communication. It is a standard of ISO.

Here **open system** is a model that allows any two different systems to communicate regardless of their underlying architecture. Mainly, it is not a protocol it is just a model.

OSI MODEL

The open system interconnection model is a layered framework. It has seven separate but interrelated layers. Each layer having unique responsibilities.

The OSI Model

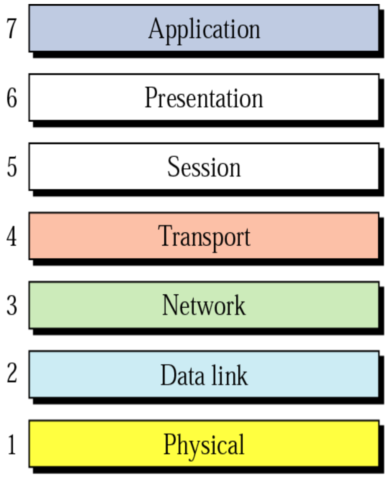


Fig 15 Seven layers of the OSI model

The OSI model shown in fig 15 is based on the proposal developed by the International Standards Organization (ISO) as a first step towards international standardization of the protocols used in the various layers. The model is called the OSI (Open System Interconnection) reference model because it deals with connecting open systems, i.e., systems that are open for communication with other systems. The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software.

The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust and interoperable.

The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems. It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network. The principles that were applied to arrive at the seven layers are as follows:

* A layer should be created where a different level of abstractionisneeded.
* Each layer should perform a well- definedfunction.
* The function of each layer should be chosen with an eye toward defining internationally standardizedprotocols.
* The layer boundaries should be chosen to minimize the information flow across the interfaces.
* The number of layers should be large enough that distinct functions need not bethrowntogether in the same layer out of necessity and small enough that the architecture does not become unwieldy.

Layered Architecture

The OSI model is composed of seven layers: Physical, Data link, Network, Transport, Session,Presentation, Application layers. Fig (iii) shows the layers involved when a message travels from A to B, it may pass through many intermediate nodes. These intermediate nodes involve only the first 3 layers of the OSI model.Within a single machine, each layer calls upon the services of the layer just below it, layer 3 for ex. Uses the services provided by layer 2 & provides services for layerBetween machines, layer X on one machine communicates with layer X on another machine. This communication is governed by an agreed upon series of rules & Conventions called protocols. The processes on each machine that communicate at a given layer are called peer – to – peer processes. Communication between machines is therefore a peer – to –peer process using the protocols appropriate to a givenlayer.

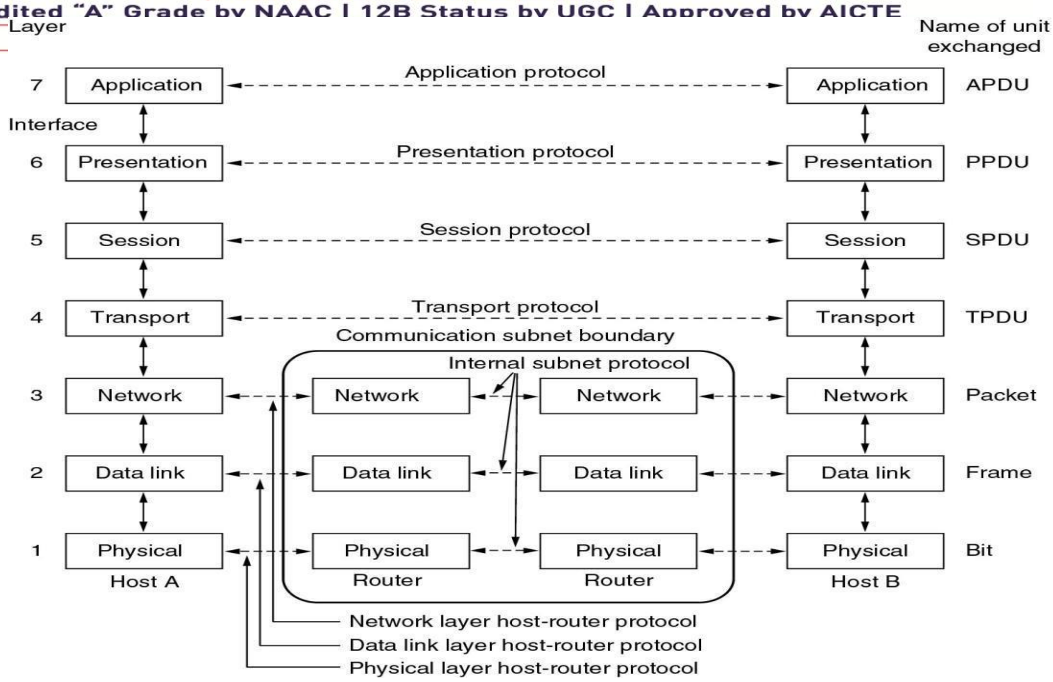


Fig 16 Interaction between layers in the OSI model

ORGANIZATION OF LAYERS

The seven layers are arranged by three sub groups.

- Network Support Layers
- User SupportLayers
- IntermediateLayer

Network Support Layers:

Physical, Datalink and Network layers come under the group. They deal with the physical aspects of the data such as electrical specifications, physical connections, physical addressing, and transport timing and reliability.

User Support Layers:

Session, Presentation and Application layers comes under the group. They deal with the interoperability between the software systems.

Intermediate Layer

The transport layer is the intermediate layer between the network support and the user support layers.

FUNCTIONS OF THE LAYERS PHYSICAL LAYER

The physical layer coordinates the functions required to transmit a bit stream over a physical medium. It deals with the mechanical and electrical specifications of the interface and the transmission medium.

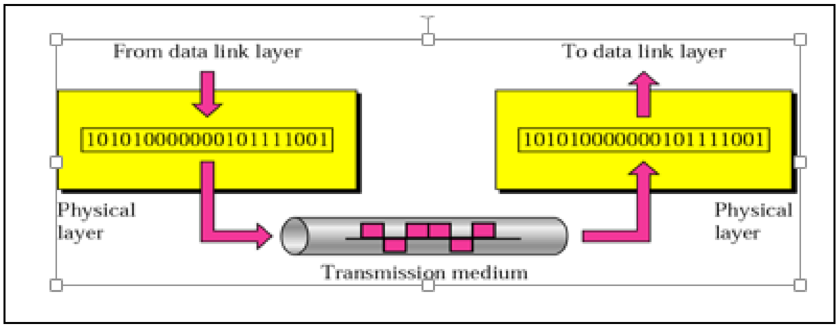


Fig 17 Physical Layer

The functions are,

1. **Physical Characteristics Of Interfaces and Media:**
    - ∗ It defines the electrical and mechanical characteristics of the interface and themedia.
    - ∗ It defines the types of transmissionmedium
2. **Representation of Bits**
    - ∗ To transmit the stream of bits they must be encoded intosignal.
    - ∗ It defines the type of encoding weather **electrical oroptical**.
3. **DataRate**
    - ∗ It defines the transmission rate i.e. the number of bits sent per second.
4. **Synchronization ofBits**
    - ∗ The sender and receiver must be synchronized at bitlevel.
5. **LineConfiguration**
    - ∗ It defines the type of connection between thedevices.
    - ∗ Two types of connectionare,

1. point to point
2. multipoint

6. **PhysicalTopology**

   ∗ It defines how devices are connected to make anetwork.

   ∗ Five topologiesare,

   1. mesh
   2. star
   3. tree
   4. bus
   5. ring

7. **Transmission Mode**

   It defines the direction of transmission between devices. Three types of transmission are,

   1. simplex
   2. halfduplex
   3. full duplex

DATALINK LAYER

Datalink layer responsible for node-to-node delivery.

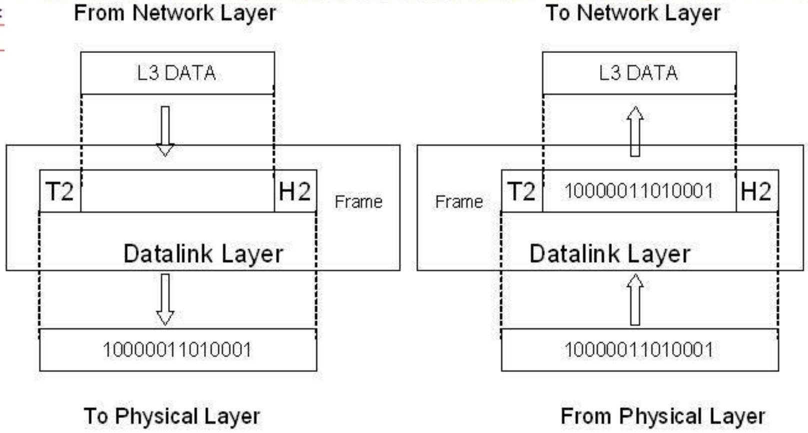


Fig 18 Data link Layer

The responsibilities of Datalink layer are,

1. **Framing**

   It divides the stream of bits received from network layer into manageable data units called **frames.**

1. **PhysicalAddressing**

   - It adds a header that defines the physical address of the sender and thereceiver.
   - If the sender and the receiver are in different networks, then the receiver address is the address of the device which connects the twonetworks.

2. **FlowControl**

   - It imposes a flow control mechanism used to ensure the data rate at the sender and the receiver should besame.

3. **ErrorControl**

   - To improve the reliability the Datalink layer adds a trailer which contains the error control mechanism like CRC, Checksumetc.

4. **AccessControl**

   - When two or more devices connected at the same link, then the Datalink layer used to determine which device has control over the link at any giventime.

NETWORK LAYER

When the sender is in one network and the receiver is in some other network then the network layer has the responsibility for the source to destinationdelivery.

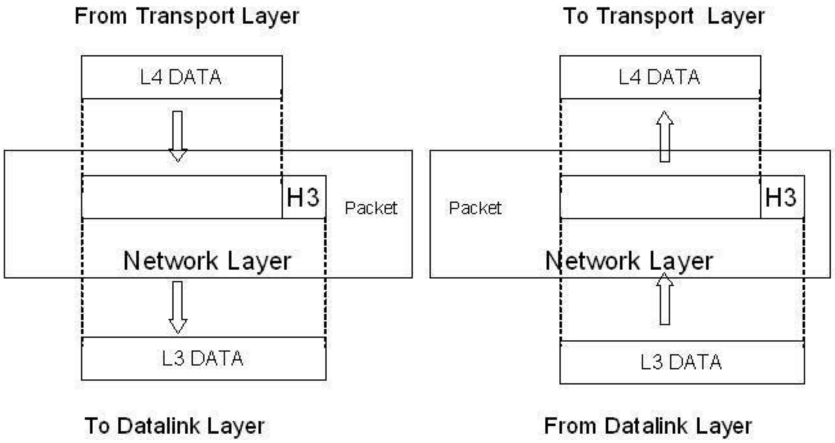


Fig 19 Network Layer

The responsibilities are,

1. **LogicalAddressing**

   ∗ If a packet passes the network boundary that is when the sender and receiver are places in different network then the network layer adds a header that defines the logical address of thedevices.

2. **Routing**

   ∗ When more than one networks connected and to form an internetwork, the connecting devices route the packet to its final destination.

   ∗ Network layer provides thismechanism.

TRANSPORT LAYER

The network layer is responsible for the end to end delivery of the entire message. It ensures that the whole message arrives in order and intact. It ensures the error control and flow control at source to destination level.

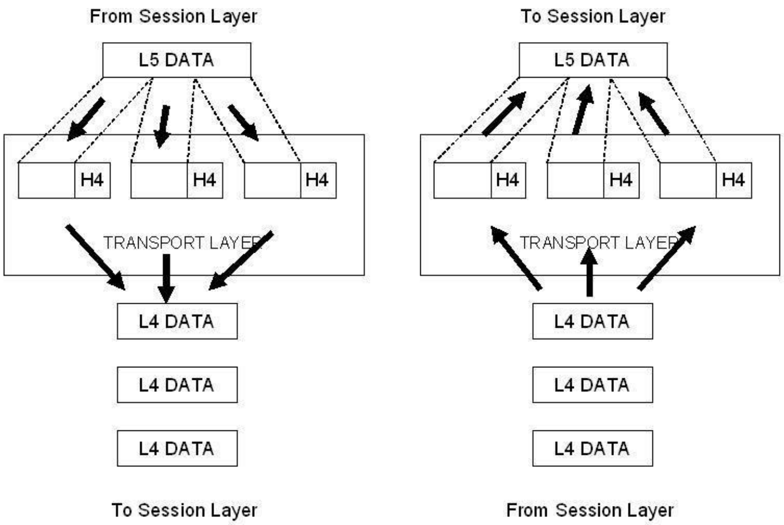


Fig 20 Transport Layer

The responsibilities are,

1. **Service pointAddressing**
   - ∗ A single computer can often run several programs at the sametime.
   - ∗ The transport layer gets the entire message to the correct process on thatcomputer.
   - ∗ It adds a header that defines the port address which used to identify the exact process on thereceiver.
2. **Segmentation and Reassembly**
   - ∗ A message is divided into manageable units called assegments.
   - ∗ Each segment is reassembled after received that information at the receiverend.
   - ∗ To make this efficient each segment contains a sequencenumber.
3. **ConnectionControl**
   - ∗ The transport layer creates a connection between the two endports.
   - ∗ It involves three steps. Theyare,

1. connectionestablishment
2. datatransmission
3. connectiondiscard

4. FlowControl

∗ Flow control is performed at end to endlevel

5. ErrorControl

∗ Error control is performed at end to endlevel.

SESSION LAYER

It acts as a dialog controller. It establishes, maintains and synchronizes the interaction between the communication devices.

The responsibilities are,

1. DialogControl

∗ The session layer allows two systems to enter into adialog.

∗ It allows the communication between thedevices.

2. Synchronization

It adds a synchronization points into a stream of bits.

PRESENTATION LAYER

The presentation layer is responsible for the semantics and the syntax of the information exchanged.

The responsibilitiesare,

1. Translation

∗ Different systems use different encodingsystems.

∗ The presentation layer is responsible for interoperability between differentsystems.

∗ The presentation layer t the sender side translates the information from the sender dependent format to a common format. Likewise, at the receiver side presentation layer translate the information from common format to receiver dependentformat.

2. **Encryption**

- To ensure security encryption/decryption isused
- Encryption means transforms the original information to another form
- Decryption means retrieve the original information from the encrypteddata

3. **Compression**

- It used to reduce the number of bits to betransmitted.

APPLICATION LAYER

The application layer enables the user to access the network. It provides interfaces between the users to the network.

The responsibilities are,

1. **Network VirtualTerminal**

It is a software version of a physical terminal and allows a user to log on to a remotehost.

2. **File Transfer, Access, andManagement**

It allows a user to access files in a remote computer, retrieve files, and manage or control files in a remotecomputer.

3. **MailServices**

It provides the basis for e-mail forwarding andstorage.

4. **DirectoryServices**

It provides distributed database sources and access for global information about various objects and services.

SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

School of Computing

Department of Computer Science and Engineering

UNIT - II

Data Communication and Computer Networks-SBS1302

UNIT II SIGNALS & ERRORS

Parallel and Serial Transmission - DTE/DCE/such as EIA-449, EIA-53O EIA-202 and x.21 interface - Interface standards - Modems - Guided Media Unguided Media - Performance - Types of Error - Error Detection - Error Corrections.

1. Parallel and Serial Transmission

Data transmission refers to the process of transferring data between two or more digital devices. Data is transmitted from one device to another in analog or digital format. Basically, data transmission enables devices or components within devices to speak to each other.Data is transferred in the form of bits between two or more digital devices. There are two methods used to transmit data between digital devices: serial transmission and parallel transmission. Serial data transmission sends data bits one after another over a single channel. Parallel data transmission sends multiple data bits at the same time over multiple channels.

Serial Transmission

When data is sent or received using serial data transmission, the data bits are organized in a specific order, since they can only be sent one after another. The order of the data bits is important as it dictates how the transmission is organized when it is received. It is viewed as a reliable data transmission method because a data bit is only sent if the previous data bit has already been received.

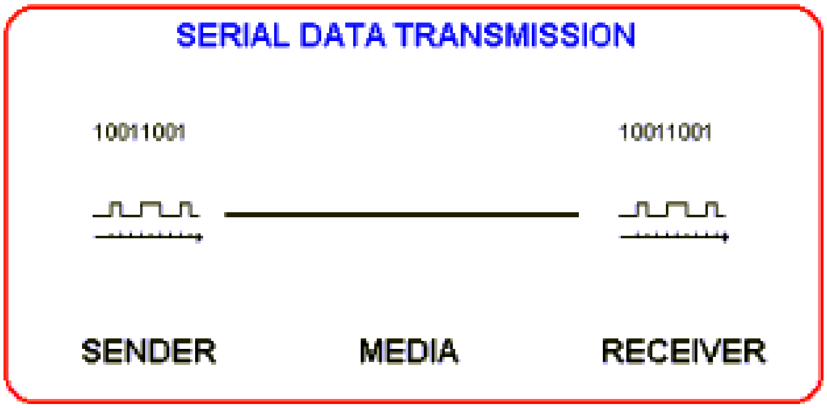


Fig 1 Serial Data Transmission

Serial transmission has two classifications: asynchronous and synchronous.

Asynchronous Serial Transmission

Data bits can be sent at any point in time. Stop bits and start bits are used between data bytes to synchronize the transmitter and receiver and to ensure that the data is transmitted correctly. The time between sending and receiving data bits is not constant, so gaps are used to provide time between transmissions.The advantage of using the asynchronous method is that no synchronization is required between the transmitter and receiver devices. It is also a more cost effective method. A disadvantage is that data transmission can be slower, but this is not always the case.

In asynchronous seria 0000000000000000l communication, the electrical interface is held in the **mark** position between characters. The start of transmission of a character is signaled by a drop in signal level to the **space** level. At this point, the receiver starts its clock. After one bit time (the start bit) come 8 bits of true data followed by one or more stop bits at the mark level.

The receiver tries to sample the signal in the middle of each bit time. The byte will be read correctly if the line is still in the intended state when the last stop bit is read.Thus the transmitter and receiver only have to have **approximately the same clock rate**. A little arithmetic will show that for a 10 bit sequence, the last bit will be interpreted correctly even if the sender and receiver clocks differ by as much as 5%. It is **relatively simple**, and therefore inexpensive. However, it has a **high overhead**, in that each byte carries at least two extra bits: a 20% loss of line bandwidth.

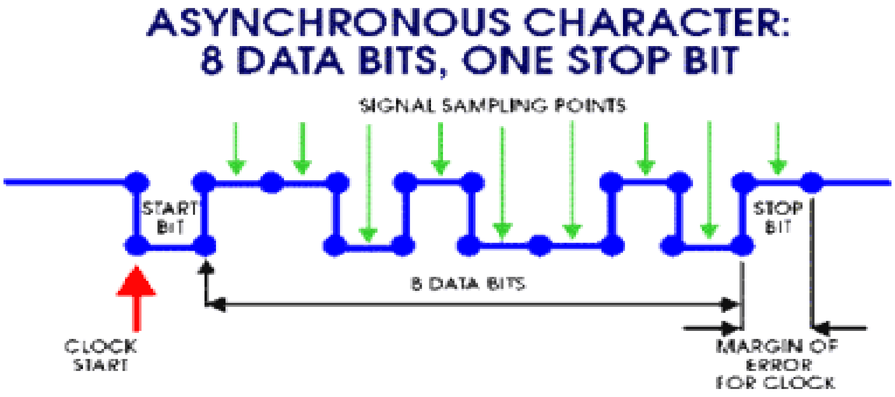


Fig 2 Asynchronous Transmission

Synchronous Serial Transmission

Data bits are transmitted as a continuous stream in time with a master clock. The data transmitter and receiver both operate using a synchronized clock frequency; therefore, start bits, stop bits, and gaps are not used. This means that data moves faster and timing errors are less frequent because the transmitter and receiver time is synced. However, data accuracy is highly dependent on timing being synced correctly between devices. In comparison with asynchronous serial transmission, this method is usually more expensive.Serial transmission is normally used for long-distance data transfer. It is also used in cases where the amount of data being sent is relatively small. It ensures that data integrity is maintained as it transmits the data bits in a specific order, one after another. In this way, data bits are received in-sync with one another.

The PS/2 mouse and keyboard implement a bidirectional synchronous serial protocol.

The bus is "**idle**" when both lines are high (open-collector). This is the only state where the keyboard/mouse is allowed begin transmitting data. The host has ultimate control over the bus and may inhibit communication at any time by pulling the Clock line low. The device (slave) always generates the clock signal. If the host wants to send data, it must first inhibit communication from the device by pulling Clock low. The host then pulls Data low and releases Clock. This is the "Request-to-Send" state and signals the device to start generating clock pulses.

Summary: Bus States

Data = high, Clock = high: *Idle state.*

Data = high, Clock = low: *Communication Inhibited.*

Data = low, Clock = high: *Host Request-to-Send*

Data is transmited 1 byte at a time:

- 1 start bit. This is always 0.
- 8 data bits, least significant bit first.
- 1 parity bit (odd parity - The number of 1's in the data bits plus the parity bit always add up to an odd number. This is used for error detection.).
- 1 stop bit. This is always 1.
- 1 acknowledge bit (host-to-device communication only)

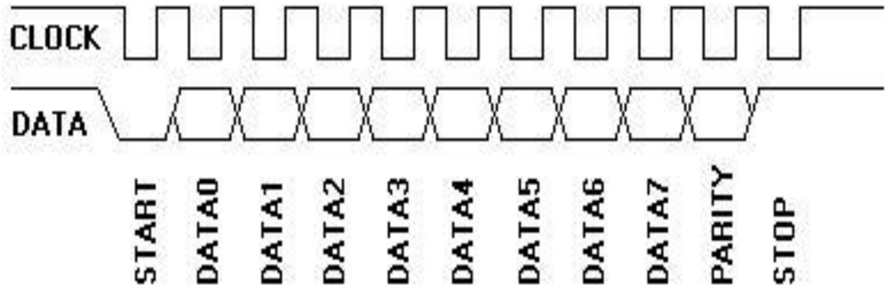


Fig 3 Synchronous Serial Transmission

Parallel transmission

When data is sent using parallel data transmission, multiple data bits are transmitted over multiple channels at the same time. This means that data can be sent much faster than using serial transmission methods.Parallel transmission (e.g. 8 bits). Each bit uses a separate wire to transfer data on a parallel link, a separate line is used as a clock signal. This serves to inform the receiver when data is available. In addition, another line may be used by the receiver to inform the sender that the data has been used, and its ready for the next data.

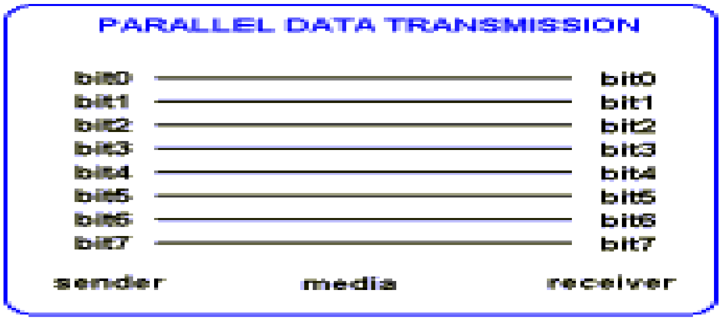


Fig 4 Parallel Transmission

Given that multiple bits are sent over multiple channels at the same time, the order in which a bit string is received can depend on various conditions, such as proximity to the data source, user location, and bandwidth availability. Two examples of parallel interfaces can be seen below. In the first parallel interface, the data is sent and received in the correct order. In the second parallel interface, the data is sent in the correct order, but some bits were received faster than others.

Advantages and Disadvantages of Using Parallel Data Transmission

The main advantages of parallel transmission over serial transmission are:

- it is easier to program;
- and data is sent faster.

Although parallel transmission can transfer data faster, it requires more transmission channels than serial transmission. This means that data bits can be out of sync, depending on transfer distance and how fast each bit loads. A simple of example of where this can be seen is with a voice over IP (VOIP) call when distortion or interference is noticeable. It can also be seen when there is skipping or interference on a video stream.

Parallel transmission is used when:

- a large amount of data is being sent;
- the data being sent is time-sensitive;
- and the data needs to be sent quickly.

A scenario where parallel transmission is used to send data is video streaming. When a video is streamed to a viewer, bits need to be received quickly to prevent a video pausing or buffering. Video streaming also requires the transmission of large volumes of data. The data being sent is also time-sensitive as slow data streams result in poor viewer experience.

2. Serial Interfaces

Serial links are simple, bidirectional links that require very few control signals. In a basic serial setup, data communications equipment (DCE) installed in a user's premises is responsible for establishing, maintaining, and terminating a connection. A modem is a typical DCE device.

A serial cable connects the DCE to a telephony network where, ultimately, a link is established with data terminal equipment (DTE). DTE is typically where a serial link terminates.

The distinction between DCE and DTE is important because it affects the cable pinouts on a serial cable. A DCE cable uses a female 9-pin or 25-pin connector, and a DTE cable uses a male 9-pin or 25-pin connector. To form a serial link, the cables are connected to each other. However, if the pins are identical, each side's transmit and receive lines are connected, which makes data transport impossible. To address this problem, each cable is connected to a null modem cable, which crosses the transmit and receive lines in the cable.

Serial Transmissions

In basic serial communications, nine signals are critical to the transmission. Each signal is associated with a pin in either the 9-pin or 25-pin connector. Table 1 lists and defines serial signals and their sources.When a serial connection is made, a serial line protocol—such as EIA-530, X.21, RS-422/449, RS-232, or V.35—begins controlling the transmission of signals across the line as follows:

The DCE transmits a DSR signal to the DTE, which responds with a DTR signal. After this handshake, the link is established and traffic can pass.

When the DTE device is ready to receive data, it sets its RTS signal to a marked state (all 1s) to indicate to the DCE that it can transmit data. (If the DTE is not able to receive data—because of buffer conditions, for example—it sets the RTS signal to all 0s.)

When the DCE device is ready to receive data, it sets its CTS signal to a marked state to indicate to the DTE that it can transmit data. (If the DCE is not able to receive data, it sets the CTS signal to all 0s.)

When the negotiation to send information has taken place, data is transmitted across the transmitted data (TD) and received data (RD) lines:

TD line—Line through which data from a DTE device is transmitted to a DCE device

RD line—Line through which data from a DCE device is transmitted to a DTE device

The name of the wire does not indicate the direction of data flow.

The DTR and DSR signals were originally designed to operate as a handshake mechanism. When a serial port is opened, the DTE device sets its DTR signal to a marked state. Similarly, the DCE sets its DSR signal to a marked state. However, because of the negotiation that takes place with the RTS and CTS signals, the DTR and DSR signals are not commonly used.The carrier detect and ring indicator signals are used to detect connections with remote modems. These signals are not commonly used.

Signal Polarity

Serial interfaces use a balanced (also called differential) protocol signaling technique. Two serial signals are associated with a circuit: the A signal and the B signal. The A signal is denoted with a plus sign (for example, DTR+), and the B signal is denoted with a minus sign (for example, DTR–). If DTR is low, then DTR+ is negative with respect to DTR–. If DTR is high, then DTR+ is positive with respect to DTR–.

By default, all signal polarities are positive, but sometimes they might be reversed. For example, signals might be mis wired as a result of reversed polarities.

Serial Clocking Modes

By default, a serial interface uses loop clocking to determine its timing source. For EIA-530 and V.35 interfaces, you can set each port independently to use one of the following clocking modes. X.21 interfaces can use only loop clocking mode. Loop clocking mode—Uses the DCE's receive (RX) clock to clock data from the DCE to the DTE.DCE clocking mode—Uses the transmit (TXC) clock, generated by the DCE specifically to be used by the DTE as the DTE's transmit clock.

Internal clocking mode—Uses an internally generated clock. The speed of this clock is configured locally. Internal clocking mode is also known as line timing. Both loop clocking mode and DCE clocking mode use external clocks generated by the DCE.

Serial Interface Clocking Modes

When an externally timed clocking mode (DCE or loop) is used, long cables might introduce a phase shift of the DTE-transmitted clock and data. At high speeds, this phase shift might cause errors. Inverting the transmit clock corrects the phase shift, thereby reducing error rates.

Serial Line Protocols

Serial interfaces support the following line protocols:

1. EIA-530
2. RS-232
3. RS-422/449
4. V.35
5. X.21

EIA-530

EIA-530 is an Electronic Industries Association (EIA) standard for the interconnection of DTE and DCE using serial binary data interchange with control information exchanged on separate control circuits. EIA-530 is also known as RS-530.The EIA-530 line protocol is a specification for a serial interface that uses a DB-25 connector and balanced equivalents of the RS-232 signals—also called V.24. The EIA-530 line protocol is equivalent to the RS-422 and RS-423 interfaces implemented on 25-pin connector.The EIA-530 line protocol supports both balanced and unbalanced modes. In unbalanced transmissions, voltages are transmitted over a single wire. Because only a single signal is transmitted, differences in ground potential can cause fluctuations in the measured voltage across the link. For example, if a 3-V signal is sent from one endpoint to another, and the receiving endpoint has a ground potential 1 V higher than the transmitter, the signal on the receiving end is measured as a 2-V signal.

Balanced transmissions use two wires instead of one. Rather than sending a single signal across the wire and having the receiving end measure the voltage, the transmitting device sends two separate signals across two separate wires. The receiving device measures the difference in voltage of the two signals (balanced sampling) and uses that calculation to evaluate the signal. Any differences in ground potential affect both wires equally, and the difference in the signals is still the same.

The EIA-530 interface supports asynchronous and synchronous transmissions at rates ranging from 20 Kbps to 2 Mbps.

RS-232

RS-232 is a Recommended Standard (RS) describing the most widely used type of serial communication. The RS-232 protocol is used for asynchronous data transfer as well as synchronous transfers using HDLC, Frame Relay, and X.25. RS-232 is also known as EIA-232.The RS-232 line protocol is very popular for low-speed data signals. RS-232 signals are carried as single voltages referred to a common ground signal. The voltage output level of these signals varies between –12 V and +12 V. Within this range, voltages between –3 V and +3 V are considered inoperative and are used to absorb line noise. Control signals are considered operative when the voltage ranges from +3 V to +25 V.

The RS-232 line protocol is an unbalanced protocol, because it uses only one wire and is susceptible to signal degradation. Degradation can be extremely disruptive, particularly when a difference in ground potential exists between the transmitting and receiving ends of a link.The RS-232 interface is implemented in a 25-pin D-shell connector and supports line rates up to 200 Kbps over lines shorter than 98 feet (30 meters).NOTERS-232 serial interfaces cannot function error-free with a clock rate greater than 200 KHz.

RS-422/449

RS-422 is a Recommended Standard (RS) describing the electrical characteristics of balanced voltage digital interface circuits that support higher bandwidths than traditional serial protocols like RS-232. RS-422 is also known as EIA-422.The RS-449 standard (also known as EIA-449) is compatible with RS-422 signal levels. The EIA created RS-449 to detail the DB-37 connector pinout and define a set of modem control signals for regulating flow control and line status.The RS-422/499 line protocol runs in balanced mode, allowing serial communications to extend over distances of up to 4,000 feet (1.2 km) and at very fast speeds of up to 10 Mbps.

Half-duplex transmission—In half-duplex transmission mode, transmissions occur in only one direction at a time. Each transmission requires a proper handshake before it is sent. This operation is typical of a balanced system in which two devices are connected by a single connection.Full-duplex transmission—In full duplex transmission mode, multiple transmissions can occur simultaneously so that devices can transmit and receive at the same time. This operation is essential when a single master in a point-to-multipoint system must communicate with multiple receivers.Multipoint transmission—RS-422/449 allows only a single master in a multipoint system. The master can communicate to all points in a multipoint system, and the other points must communicate with each other through the master.

V.35

V.35 is an ITU-T standard describing a synchronous, Physical Layer protocol used for communications between a network access device and a packet network. V.35 is most commonly used in the United States and Europe.The V.35 line protocol is a mixture of balanced (RS-422) and common ground (RS-232) signal interfaces. The V.35 control signals DTR, DSR, DCD, RTS, and CTS are single-wire common ground signals that are essentially identical to their RS-232 equivalents. Unbalanced signaling for these control signals is sufficient, because the control signals are mostly constant, varying at very low frequency, which makes single-wire transmission suitable. Higher frequency data and clock signals are sent over balanced wires.

X.21

X.21 is an ITU-T standard for serial communications over synchronous digital lines. The X.21 protocol is used primarily in Europe and Japan.The X.21 line protocol is a state-driven protocol that sets up a circuit-switched network using call setup. X.21 interfaces use a 15-pin connector with the following eight signals:

Signal ground (G)—Reference signal used to evaluate the logic states of the other signals. This signal can be connected to the protective earth (ground).

DTE common return (Ga)—Reference ground signal for the DCE interface. This signal is used only in unbalanced mode.

Transmit (T)—Binary signal that carries the data from the DTE to the DCE. This signal can be used for data transfer or in call-control phases such as Call Connect or Call Disconnect.

Receive (R)—Binary signal that carries the data from the DCE to the DTE. This signal can be used for data transfer or in call-control phases such as Call Connect or Call Disconnect.

Control (C)—DTE-controlled signal that controls the transmission on an X.21 link. This signal must be on during data transfer, and can be on or off during call-control phases.

Indication (I)—DCE-controlled signal that controls the transmission on an X.21 link. This signal must be on during data transfer, and can be on or off during call-control phases.

Signal Element Timing (S)—Clocking signal that is generated by the DCE. This signal specifies when sampling on the line must occur.

Byte Timing (B)—Binary signal that is on when data or call-control information is being sampled. When an 8-byte transmission is over, this signal switches to off.

Transmissions across an X.21 link require both the DCE and DTE devices to be in a ready state, indicated by an all 1s transmission on the T and R signals.

3. Modem

Modem is abbreviation for Modulator – Demodulator. Modems are used for data transfer from one computer network to another computer network through telephone lines. The computer network works in digital mode, while analog technology is used for carrying massages across phone lines.

Modulator converts information from digital mode to analog mode at the transmitting end and demodulator converts the same from analog to digital at receiving end. The process of converting analog signals of one computer network into digital signals of another computer network so they can be processed by a receiving computer is referred to as digitizing.

When an analog facility is used for data communication between two digital devices called Data Terminal Equipment (DTE), modems are used at each end. DTE can be a terminal or a computer.

DTE can be a terminal or a computer.

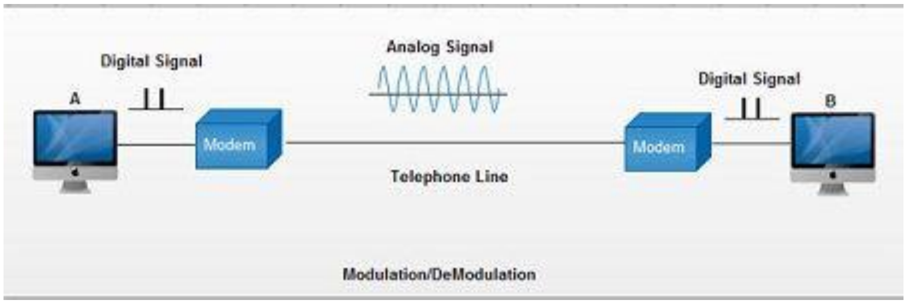
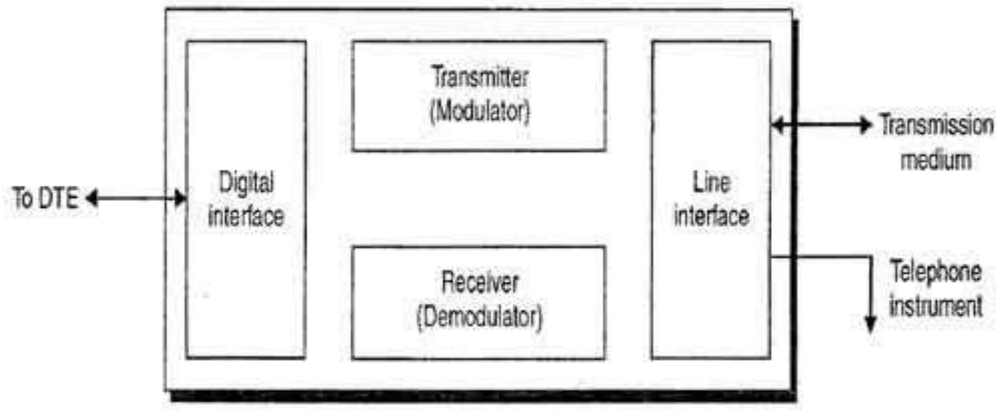


Fig 5 Modulation and Demodulation

The modem at the transmitting end converts the digital signal generated by DTE into an analog signal by modulating a carrier. This modem at the receiving end demodulates the carrier and hand over the demodulated digital signal to the DTE.



Building blocks of a modem

Fig 6 Building blocks of modem

The transmission medium between the two modems can be dedicated circuit or a switched telephone circuit. If a switched telephone circuit is used, then the modems are connected to the local telephone exchanges. Whenever data transmission is required connection between the modems is established through telephone exchanges.

Ready to Send

To begin with the Data Terminal Equipment or DTE (better known as a computer) sends a Ready To Send or RTS signal to the Data Communication Equipment or DCE (better known as a modem). This is sometimes known as a wakeup call and results in the modem sending a Data Carrier Detect or DCD signal to the receiving modem. There then follows a series of signals passed between the two until the communication channel has been established. This process is known as handshaking and helps to explain why, even now, some companies like CompuServe use the symbol of two hands grasping each other to mean being on-line. Of course, after that all it takes is for the second modem to send a Data Set Ready or DSR signal to its computer and wait for the Data Terminal Ready or DTR reply. When that happens the first modem sends a Clear To Send or CTS signal to the computer that started the whole process off and data can then be transmitted. It is as simple as that.

Types of Modems

- Modems can be of several types and they can be categorized in a number of ways.
- Categorization is usually based on the following basic modem features:

1. Directional capacity: half duplex modem and full duplex modem.

2. Connection to the line: 2-wire modem and 4-wire modem.

3. Transmission mode: asynchronous modem and synchronous modem.

Half duplex and full duplex Modems

Half duplex

1. A **half duplex modem** permits transmission in one direction at a time.

2. If a carrier is detected on the line by the modem, I gives an indication of the incoming carrier to the DTE through a control signal of its digital interface.

3. As long as they camel' IS being received; the modem does not give permission to the DTE to transmit data.

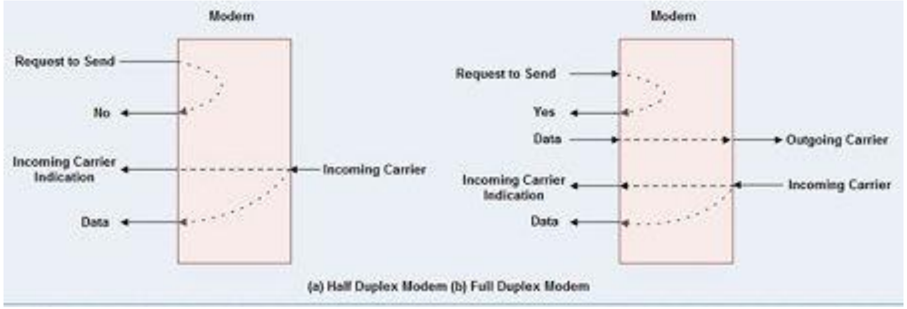


Fig 7 a) Half duplex modem b) Full duplex modem

Full duplex

• A **full duplex modem** allows simultaneous transmission in both directions.

• Therefore, there are two carriers on the line, one outgoing and the other incoming. **Wire and 4-wire Modems**

• The line interface of the modem can have a 2-wire or a 4-wire connection to transmission medium. 4-wire Modem

• In a 4-wire connection, one pair of wires is used for the outgoing carrier and the other pair is used for incoming carrier.

• Full duplex and half duplex modes of data transmission are possible on a 4- wire connection.

• As the physical transmission path for each direction is separate, the same carrier frequency can be used for both the directions.

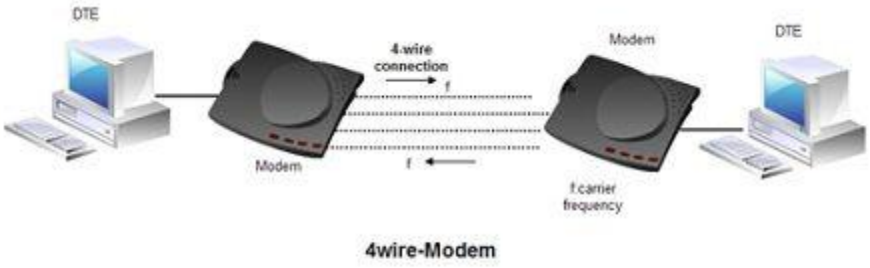


Fig 8 4-Wire modem

2-wire Modem

• 2-wire modems use the same pair of wires for outgoing and incoming carriers. A leased 2-wireconrlection is usually cheaper than a 4-wire connection as only one pair of wires is extended to the subscriber's premises. The data connection established through telephone exchange is also a 2-wire connection. In 2-wire modems, half duplex mode of transmission that uses the same frequency for the incoming and outgoing carriers can be easily implemented. For full duplex mode of operation, it is necessary to have two transmission channels, one for transmit direction and the other for receive direction. This is achieved by frequency division multiplexing of two different carrier frequencies. These carriers are placed within the bandwidth of the speech channel.

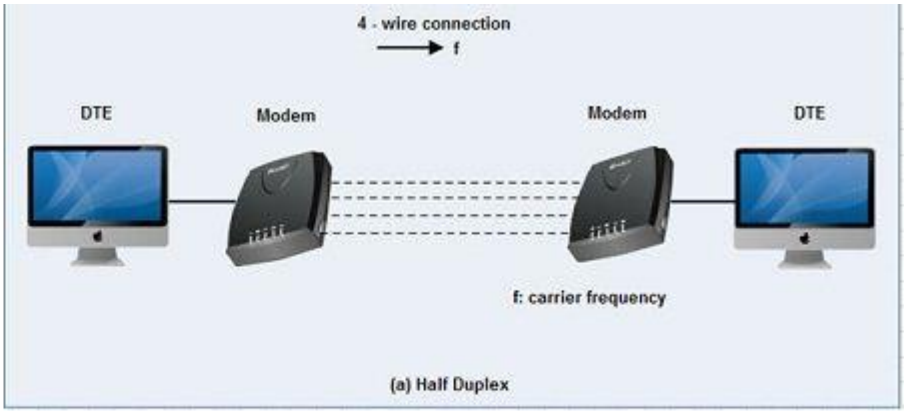


Fig 9 Half Duplex

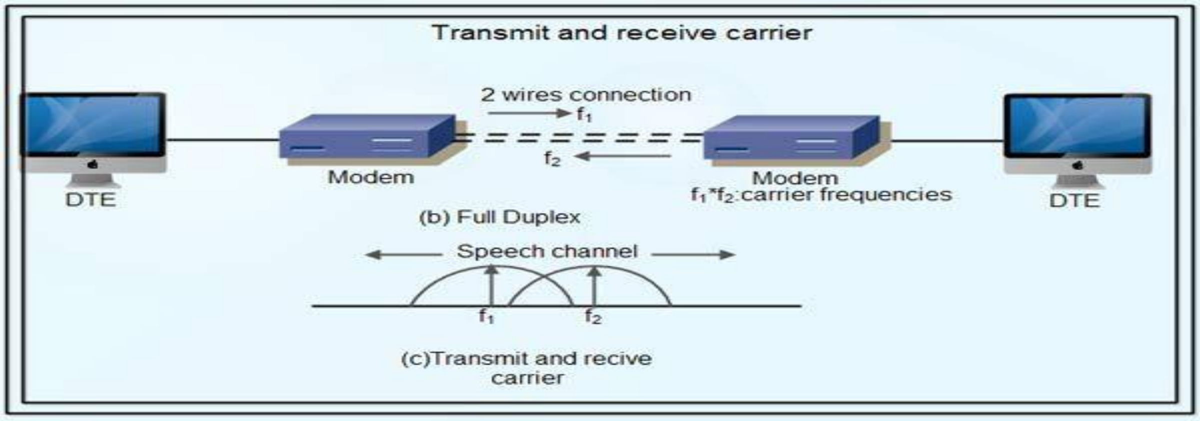

Transmit and receive carrier
2 wires connection
f1
f2
DTE
Modem
Modem
f1*f2:carrier frequencies
DTE
(b) Full Duplex
Speech channel
f1
f2
(c)Transmit and recive carrier

Fig 10 a) Full Duplex b) Transmit and receive carrier

Asynchronous & Synchronous Modems

Asynchronous Modem

Asynchronous modems can handle data bytes with start and stop bits. There is no separate timing signal or clock between the modem and the DTE. The internal timing pulses are synchronized repeatedly to the leading edge of the start pulse .

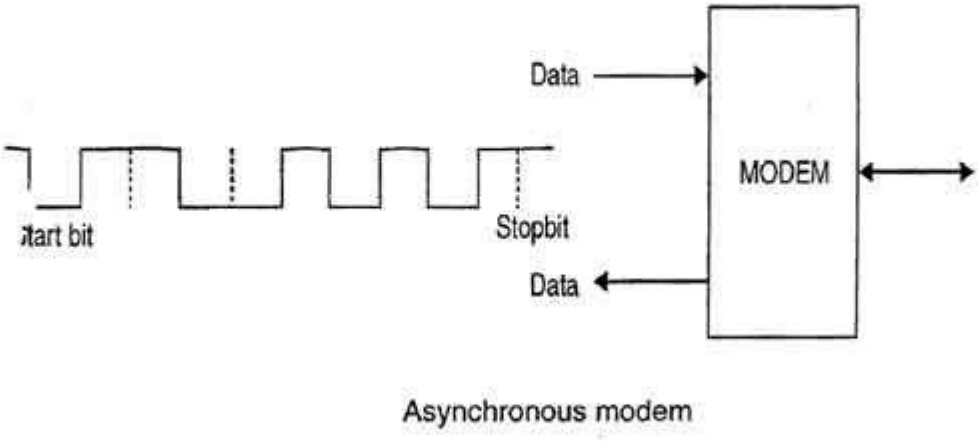


Fig 11 Asynchronous modem

Synchronous Modem

Synchronous modems can handle a continuous stream of data bits but requires a clock signal. The data bits are always synchronized to the clock signal. There are separate clocks for the data bits being transmitted and received. For synchronous transmission of data bits, the DTE can use its internal clock and supply the same to the modem.

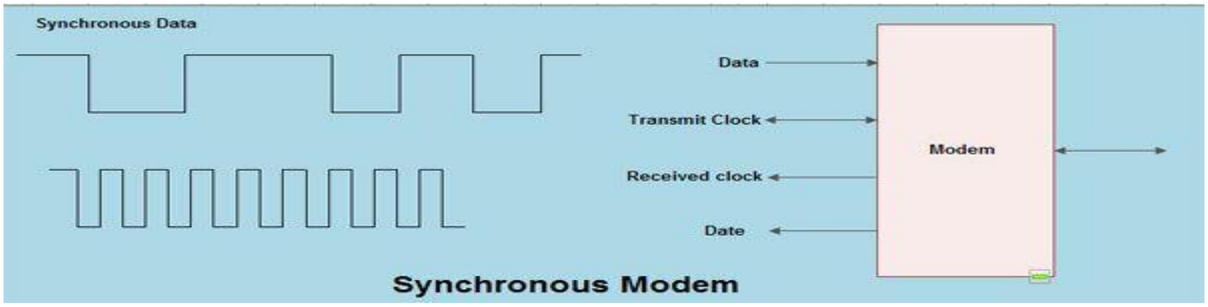


Fig 12 Synchronous Modem

Modulation techniques used for Modem:

The basic modulation techniques used by a modem to convert digital data to analog signals are :

- Amplitude shift keying (ASK).
- Frequency shift keying (FSK).
- Phase shift keying (PSK).
- Differential PSK (DPSK).

These techniques are known as the binary continuous wave (CW) modulation.

- Modems are always used in pairs. Any system whether simplex, half duplex or full duplex requires a modem at the transmitting as well as the receiving end.
- Thus a modem acts as the electronic bridge between two worlds - the world of purely digital signals and the established analog world.

4. Transmission Media

A **transmission medium** (plural *transmission media*) is a material substance (solid, liquid, gas, or plasma) which can propagate energy waves. For example, the transmission medium for sound received by the ears is usually air, but solids and liquids may also act as transmission media for sound.

Transmission media are the physical pathways that connect computers, other devices, and people on a network. Each transmission medium requires specialized network hardware that is compatible with that medium, and most networks need to use combination of transmission media types selected based on the network's needs and prevailing conditions. The term **transmission medium** can also refer to the technical device which employs the material substance to transmit or guide the waves. Thus an optical fiber or a copper cable can be referred to as a transmission medium. The absence of a material medium (the vacuum of empty space) can also be thought of as a transmission medium for electromagnetic waves such as light and radio waves. While material substance is not required for electromagnetic waves to propagate, such waves are usually affected by the transmission media through which they pass, for instance by absorption or by reflection or refraction at the interfaces between media.

A transmission medium can be classified as a:

- Linear medium, if different waves at any particular point in the medium can be superposed;
- Bounded medium, if it is finite in extent, otherwise unbounded medium;
- Uniform medium or homogeneous medium, if its physical properties are unchanged at different points;
- Isotropic medium, if its physical properties are the same in different directions.

Types of Transmission media:

The means through which data is transformed from one place to another is called transmission or communication media. There are two categories of transmission media used in computer communications.

- **GUIDEDMEDIA**
- **UNGUIDEDMEDIA**

5. Guided Media:

Bounded media are the physical links through which signals are confined to narrow path. These are also called guide media. Bounded media are made up oa external conductor (Usually Copper) bounded by jacket material. Bounded media are great for LABS because they offer high speed, good security and low cast. However, some time they cannot be used due distance communication. Three common types of bounded media are used of the data transmission. There are several types of cable which are commonly used with LANs. In some cases, a network will utilize only one type of cable, other networks will use a variety of cable types. The type of cable chosen for a network is related to the network's topology, protocol, and size. Understanding the characteristics of different types of cable and how they relate to other aspects of a network is necessary for the development of a successful network.

a. Unshielded Twisted Pair (UTP)Cable
b. Shielded Twisted Pair (STP)Cable
c. Coaxial Cable
d. Fiber Optic Cable

TWISTED PAIR CABLE :

e. The most popular network cabling is Twisted pair. It is light weight, easy to install, inexpensive and support many different types of network. It also supports the speed of **100 mps.** Twisted pair cabling is made of pairs of solid or stranded copper twisted along each other. The number of pairs in the cable depends on the type. The copper core is usually **22-AWG or 24-AWG, as** measured on the American wire gauge standard.

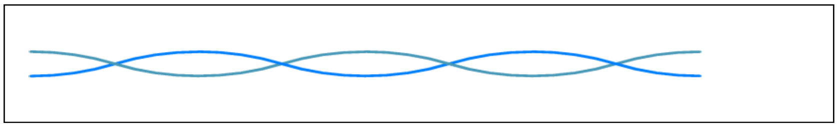


Fig 13 Twisted pair wire

There are two types of twisted pairs cabling

1. **Unshielded twisted pair(UTP)**

2. **Shielded twisted pair(STP)**

Unshielded Twisted Pair (UTP)Cable

Twisted pair cabling comes in two varieties: shielded and unshielded. Unshielded twisted pair (UTP) is the most popular and is generally the best option for school networks.

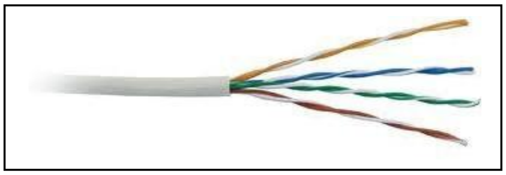


Fig 14 Unshielded Twisted Pair

The quality of UTP may vary from telephone-grade wire to extremely high-speed cable. The cable has four pairs of wires inside the jacket. Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices.

The tighter the twisting, the higher the supported transmission rate and the greater the cost per foot. The EIA/TIA (Electronic Industry Association / Telecommunication Industry Association) has established standards of UTP and rated five categories of wire.

Table 1 Categories of Unshielded Twisted Pair

Type	**Use**
Category 1	Voice Only (Telephone Wire)
Category 2	Data to 4 Mbps (LocalTalk)
Category 3	Data to 10 Mbps (Ethernet)
Category 4	Data to 20 Mbps (16 Mbps Token Ring)
Category 5	Data to 100 Mbps (Fast Ethernet)

CHARACTERISTICS_

- Easy to install
- High speed capacity
- High attenuation
- Effective to EMI
- 100 meter limit

ADVANTAGES :

- Easy installation
- Capable of high speed for LAN
- Low cost

DISADVANTAGES :

- Short distance due to attenuation

Unshielded Twisted Pair Connector Shielded twisted pair (STP)

It is similar to UTP but has a mesh shielding that's protects it from EMI which allows for higher transmission rate. IBM has defined category for STP cable.

Type 1: STP features two pairs of 22-AWG

Type 2: This type include type 1 with 4 telephone pairs

Type 3: This type feature two pairs of standard shielded 26-AWG

Type 4: This type of STP consists of 1 pair of standard shielded 26-AWG

Type 5: This type consist of shielded 26-AWG wire

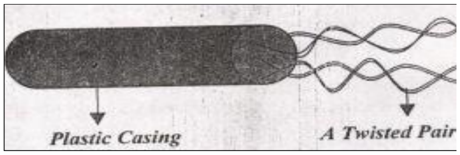


Fig 15 Twisted Pair

CHARACTERISTICS:

□ Medium cost

□ Easy to install

□ Higher capacity than UTP

□ Higher attenuation, but same as UTP

□ Medium immunity from EMI

□ 100 meter limit

ADVANTAGES :

□ Faster than UTP and coaxial &Shielded

DISADVANTAGES :

- More expensive than UTP and coaxial
- More difficult installation
- High attenuation rate

The standard connector for unshielded twisted pair cabling is an RJ-45 connector. This is a plastic connector that looks like a large telephone-style connector (See fig. 2.2). a slot allows the RJ-45 to be inserted only one way. RJ stands for Registered Jack, implying that the connector follows a standard borrowed from the telephone industry. This standard designates which wire goes with each pin inside the connector.

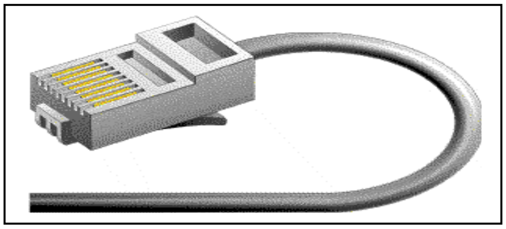


Fig 16 RJ-45

Shielded Twisted Pair (STP) Cable

A disadvantage of UTP is that it may be susceptible to radio and electrical frequency interference. Shielded twisted pair |(STP) is suitable for environments with electrical interference; however, the extra shielding can make the cables quite bulky. Shielded twisted pair is often used on networks using Token Ring topology.

Coaxial Cable

Coaxial cabling has a single copper conductor at its center. A plastic layer provides insulation between the center conductor and the braided metal shield (See fig. 3). The metal shield helps to block any outside interference from fluorescent lights, motors, and other computers.

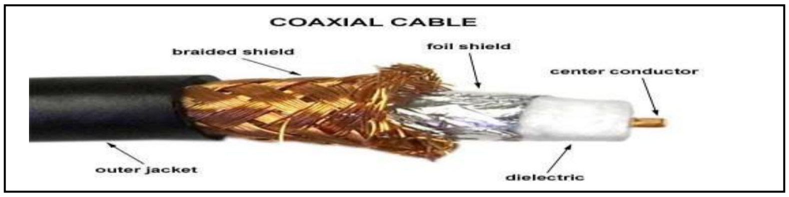


Fig 17 Coaxial Cable

Although coaxial cabling is difficult to install, it is highly resistant to signal interference. In addition, it can support grater cable lengths between network devices than twisted pair cable. The two types of coaxial cabling are thick coaxial and thin coaxial.

Thin coaxial cable is also referred to as thinnet. 10base2 refers to the specifications for thin coaxial cable carrying Ethernet signals. The 2 refers to the approximate maximum segment length being 200 meters. In actual fact the maximum segment length is 185 meters. Thin coaxial cable is popular in school networks, especially linear bus networks.

Thick coaxial cable is also referred to as thicknet. 10base refers to the specifications for thick coaxial cable carrying Ethernet signals. The 5 refers to the maximum segment length being 500 meters. Thick coaxial cable has an extra protective plastic cover that helps keep moisture away from the center conductor. This makes thick coaxial a great choice when running longer lengths in a linear bus network. One disadvantage of thick coaxial is that it does not bend easily and is difficult to install.

Here the most common coaxial standards

- 50-Ohm RG-7 or RG-11 : used with thick Ethernet.
- 50-Ohm RG-58 : used with thin Ethernet
- 75-Ohm RG-59 : used with cable television
- 93-Ohm RG-62 : used with ARCNET.

CHARACTERISTICS :

- Low cost
- Easy to install
- Up to 10Mbpscapacity
- Medium immunity form EMI
- Medium of attenuation

ADVANTAGES :

- Inexpensive
- Easy to wire
- Easy to expand
- Moderate level of EMI immunity

DISADVANTAGE :

- Single cable failure can take down an entire network

Coaxial Cable Connectors

The most common type of connector used with coaxial cables is the Bayone-Neill-Concelmnan (BNC) connector (See fig. 4). Different types of adapters are available for BNC connectors, including a T-connector, barrel connector, and a terminator. Connectors on the cable are the weakest points in any network. To help avoid problems with your network, always use the BNC connectors that crimp, rather than screw, onto the cable.

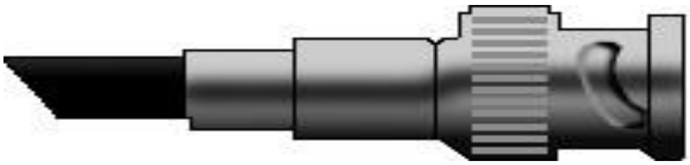


Fig 18 BNC Connector

Fiber Optic Cable

Fiber optic cabling consists of a center glass core surrounded by several layers of protective materials. It transmits light rather than electronic signals eliminating the problem of electrical interference.

This makes it ideal for certain environments that contain a large amount of electrical interference. It has also made it the standard for connecting networks between buildings, due to its immunity to the effects of moisture and lighting.

Fiber optic cable has the ability to transmit signals over much longer distances than coaxial and twisted pair. It also has made it the standard for connecting networks between buildings, due to its immunity to the effects of moisture and lighting.

Fiber optic cable has the ability to transmit signals over mush longer distances than coaxial and twisted pair. It also has the capability to carry information at vastly greater speeds. This capacity broadens communication possibilities to include services such as video conferencing and interactive services. The cost of fiber optic cabling is comparable to copper cabling; however it is more difficult to install and modify. 10BaseF refers to the specifications for fiber optic cable carrying Ethernet signals.

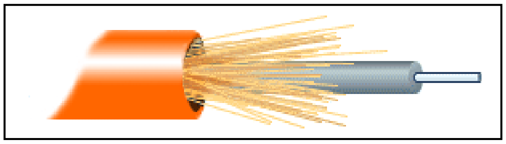


Fig 19 Fiber Optic Cable

Facts about fiber optic cables:

- □ Outer insulating jacket is made of Teflon or PVC.
- □ Kevlar fiber helps to strengthen the cable and prevent breakage.
- □ A plastic coating is used to cushion the fiber center.
- □ Center (core) is made of glass or plastic fibers.

CHARACTERISTICS:

- Expensive
- Very hard to install
- Capable of extremely high speed
- Extremely low attenuation
- No EMI interference

ADVANTAGES :

- Fast
- Low attenuation
- No EMI interference

DISADVANTAGES :

- Very costly
- Hard to install

Fiber Optic Connector

The most common connector used with fiber optic cable is an ST connector. It is barrel shaped, similar to a BNC connector. A newer connector, the SC, is becoming more popular. It has a squared face and is easier to connect in a confined space.

Table 2 Ethernet Cable Summary

Specification	Cable Type	Maximum length
10BaseT	Unshielded Twisted Pair	100 meters
10Base2	Thin Coaxial	185 meters
10Base5	Thick Coaxial	500 meters
10BaseF	Fiber Optic	2000 meters
100BaseT	Unshielded Twisted Pair	100 meters
100BaseTX	Unshielded Twisted Pair	220 meters

Installing Cable Guidelines

When running cable, it is best to follow a few simple rules:

- Always use more cable than you need. Leave plenty of slack.
- Test every part of a network as you install it. Even if it is brand new, it may have problems that will be difficult to isolate later.
- Stay at least 3 feet away from fluorescent light boxes and other sources of electrical interference.

- If it is necessary to run cable across the floor, cover the cable with cable protectors.
- Label both ends of each cable.
- Use cable ties (not tape) to keep cables in the same location together.

Where to put the cable?

The use of the surface allows cables to run along the outer edges of common floors covered by metal conduits that are attached at the room's floorboards.

Advantage:

This method is popular because it provides protection from electromagnetic interference.

Disadvantages:

- They are difficult to move or modify if a network expands or changes.
- Cable can also be installed under floors or over ceilings.
- Under floor cabling is usually housed in steel ducts or trenches.

Advantages:

- It is difficult to tap and is resistant to breaks and cuts.
- Over-ceiling cabling competes with air conditioning, lighting, and power conducts that some times squeeze out this popular, inexpensive emethod.

Who is responsible forcabling?

- Telephone installers
- LANi nstaller
- Network Manager

Often, a network manager must work with:

- LAN vendors
- Cabling vendors
- Cable installation firms

- Individual users
- Building owners or managers

As far as cabling is concerned, his / her job is to be responsible for:

- Installing
- Moving
- Changing
- Inventorying
- Regularly testing cables

6. UNBOUNDED MEDIA Or Unguided

Unguided transmission media are methods that allow the transmission of data without the use of physical means to define the path it takes. Unguided media provide a means for transmitting electromagnetic waves but do not guide them; examples are propagation through air, vacuum and seawater. For unguided media, the bandwidth of signal produced by the transmitting antenna is more important than the medium in determining transmission characteristics. One key property of signals transmitted by antenna is directionality. Unguided transmission media is data signals that flow through the air. They are not guided or bound to a channel to follow.

Unguided media transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication. Signals are normally broadcast through free space and thus are available to anyone who has a device receiving them. Unguided signals can travel from the source to destination in several ways: ground propagation, sky propagation, and line-of-sight propagation.

In ground propagation, radio waves travel through the lowest portion of the atmosphere, hugging the earth. These low-frequency signals emanate in all directions from the transmitting antenna and follow the curvature of the planet. Distance depends on the amount of power in the signal: The greater the power, the greater the distance. Ground waves have carrier frequencies up to 2 MHz. AM radio is an example of ground wave propagation.In sky propagation, higher frequency radio waves radiate upward into the ionosphere (the layer of atmosphere where the particles exist as ions) where they are reflected back to the earth. This

type of transmission allows for greater distances with lower output power.

It is sometimes called double hop propagation. It operates in the frequency range of 30 – 85

MHz. Because it depends on the earth's ionosphere, it changes with the weather and time of day. The signal bounces off of the ionosphere and back to the earth. Ham radios operate in this range. Other books called this Ionospheric propagation.

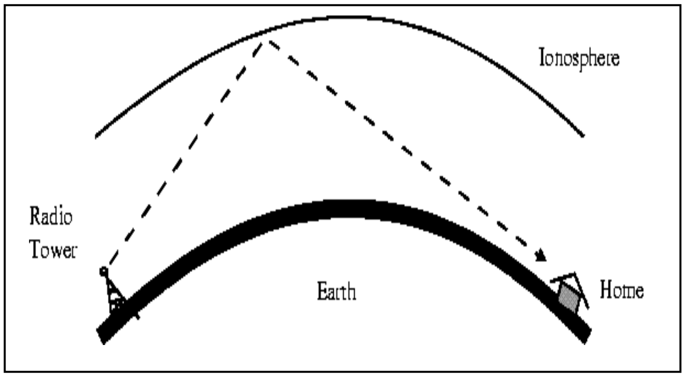


Fig 20 Ionospheric Propagation

In line-of-sight propagation, very high-frequency signals are transmitted in straight lines directly from antenna to antenna. Antennas must be directional, facing each other and either tall enough or close enough together not to be affected by the curvature the earth. Line-of-sight propagation is tricky because radio transmission cannot be completely focused.

It is sometimes called space waves or tropospheric propagation. It is limited by the curvature of the earth for ground-based stations (100 km, from horizon to horizon). Reflected waves can cause problems. Examples are: FM radio, microwave and satellite.

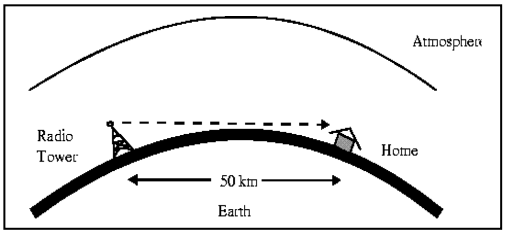


Fig 21 Line-of-sight Propagation

The section of the electromagnetic spectrum defined as radio waves and microwaves is divided into eight ranges, called bands, each regulated by government authorities. These bands are rated from very low frequency (VLF) to extremely high frequency (EHF).

We can divide wireless transmission into three broad groups: radio waves, microwaves, and infrared waves.

Examples of Unguided media are:

a. microwave
b. radio waves
c. infrared waves
d. Satellites

Radio Waves

Electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called radio waves. Radio waves are omni directional. When antenna transmits radio waves, they are propagated in all directions. This means that the sending and receiving antennas do not have to be aligned. A sending antenna sends waves that can be received by any receiving antenna.

The omni directional property has a disadvantage too. The radio waves transmitted by one antenna are susceptible to interference by another antenna that may send signals using the same frequency or band.

Radio waves, particularly those of low and medium frequencies, can penetrate walls. This characteristic can be both an advantage and disadvantage. It is an advantage because, for example, an AM radio can receive signals inside a building. It is a disadvantage because we cannot isolate a communication to just inside or outside a building.

Radio is the transmission of signals by modulation of electromagnetic waves with frequencies below those of visible light. Electromagnetic radiation travels by means of oscillating electromagnetic fields that pass through the air and the vacuum of space. Information is carried by systematically changing (modulating) some property of the radiated waves, such as amplitude, frequency, phase, or pulse width. When radio waves pass an electrical conductor, the oscillating fields induce an alternating current in the conductor. This can be detected and transformed into sound or other signals that carry information.

Characteristics:

- Directed Waves
- Noise Concurrency

- Radio Wave's Directness
- Unlimited Range
- Interference

ADVANTAGES :

- Can carry a message instantaneously over a wide area.
- Aerials to receive them are simpler than for microwaves.
- Wires are not needed as they travel through air, thus, a cheaper form of communication.

DISADVANTAGES:

- The range of frequencies that can be accessed by existing technology is limited, so there is a lot of competition amongst companies for the use of the frequencies.
- Travel in a straight line, so repeater stations may be needed.

Microwaves

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

Microwaves are unidirectional. When an antenna transmits microwave waves, 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. The following describes some characteristics of microwave propagation:

- Microwave propagation is line-of-sight. Since towers with the mounted antennas need to be in direct sight of each other. This also set a limit on the distance between stations depending on the local geography. Towers that are far apart need to be very tall. The curvature of the earth as well as other blocking obstacles does not allow two short towers to communicate by using microwaves. Typically the line of sight due to the Earth’s curvature is only 50 km to the horizon. Repeaters are often needed for long-distance communication.
- Very high frequency microwaves cannot penetrate walls. This characteristic can be a

disadvantage if receivers are inside the buildings.

- The microwave band is relatively wide, almost 299 GHz. Therefore wider sub bands can be assigned, and a high data rate is possible.
- Use of certain portions of the band requires permission from authorities.

Advantages :

- No cables needed
- Multiple channels available
- Wide bandwidth

Disadvantages:

- Line-of-sight will be disrupted if any obstacle, such as new buildings, are in theway
- Signal absorption by the atmosphere. Microwaves suffer from attenuation due to atmospheric conditions.
- Towers are expensive to build

Infrared Waves

Infrared waves, with frequencies from 300 GHz to 400 THz (wavelengths from 1 mm to 770 mm), can be used for short-range communication. Infrared waves, having high frequencies, cannot penetrate walls. This advantageous characteristic prevents interference between one system and another; a short-range communication system in one room cannot be affected by another system in the next room. When we use our infrared remote control, we do not interfere with the use of the remote of our neighbors. However, this same characteristic makes infrared signals useless for long-range communication. In addition, we cannot use infrared waves outside a building because the sun's rays contain infrared waves that can interfere with the communication.

Infrared (IR) light is electromagnetic radiation with a wavelength between 0.7 and 300 micrometers, which equates to a frequency range between approximately 1 and 430 THz.

IR wavelengths are longer than that of visible light, but shorter than that of terahertz radiation microwaves. Bright sunlight provides an irradiance of just over 1 kilowatt per square meter at sea level. Of this energy, 527 watts is infrared radiation, 445 watts is visible light, and 32 watts is ultraviolet radiation.

Advantages :

- Many things are controlled by infrared.
- Sensors are invisible to the naked eye.
- They are very reliable.

Disadvantages:

- Most infrared sensors must be lined up or they will not work

Satellite

Satellites are transponders (units that receive on one frequency and retransmit on another) that are set in geostationary orbits directly over the equator. These geostationary orbits are 36, 000 km from the Earths's surface. At this point, the gravitational pull of the Earth and the centrifugal force of Earth's rotation are balanced and cancel each other out. Centrifugal force is the rotational force placed on the satellite that wants to fling it out into the space.

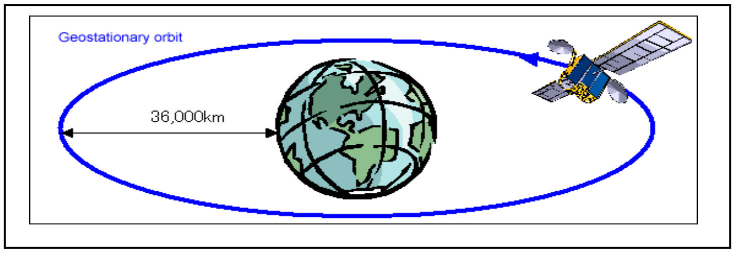


Fig 22 Satellite Communication

The uplink is the transmitter of data to the satellite. The downlink is the receiver of data. Uplinks and downlinks are also called Earth stations because they are located on the Earth. The footprint is the "shadow" that the satellite can transmit to, the shadow being the area that can receive the satellite's transmitted signal.

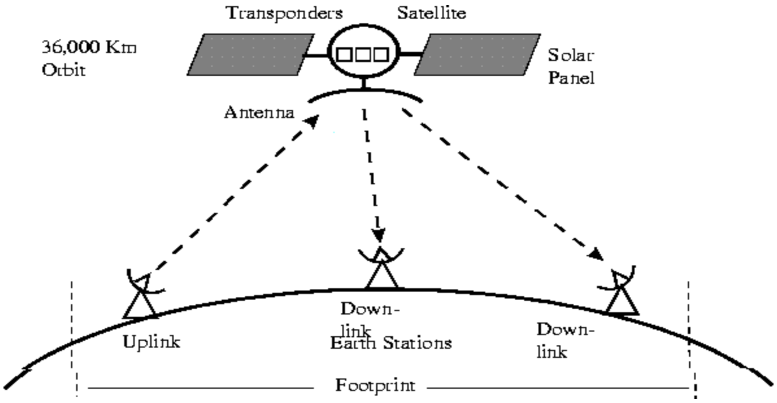


Fig 23 Uplink and Downlink

Advantages of satellite communication :

Availability

The biggest advantage of satellite Internet access is its availability compared to other Internet connection types. Satellite Internet access is a way for those who do not have access to terrestrial broadband connections such as cable or DSL to have access to high-speed Internet access. Satellite also is one of the only ways to receive Internet service in areas where telephone lines are not available.

Speed

Satellite Internet access is much faster than dial-up, with entry-level service tiers typically providing approximately 1 mbps download speeds--nearly 18 times faster than a dial- up modem. Faster speeds are generally available at higher service tiers. In general, the highest speeds available to home satellite Internet customers are slightly slower than the highest speeds offered by cable and DSL providers. Additionally, many satellite providers limit the amount of data that can be downloaded during short time periods to curb frequent large file transfers.

Latency

Satellite Internet connections are high-latency, meaning that a great deal of time is required for packets of information to travel to the satellite and back. The total delay can amount to about one second from the time that you send a request to the Internet to the time that a reply is received. Satellite Internet providers use various technologies to make this delay less noticeable to the end user and create an acceptable experience for browsing the Web. However, the latency makes a satellite Internet connection unsuitable for high-speed gaming.

Reliability

Home-based satellite Internet connections are generally no less reliable than terrestrial broadband. However, all satellite communication is subject to interruption during periods of heavy snow or rainfall. Talk to other customers about their experiences if you live in an area where either of these are common. The likelihood of weather-related interruptions is lessened with a larger satellite dish, which some providers offer.

Cost

The equipment costs several hundred dollars to purchase, and some types of installations incur additional fees. Additionally, the monthly cost for satellite Internet tends to be slightly higher than the cost of cable or DSL. There are ways of reducing the up-front cost. The equipment can be leased rather than purchased, and discounts or rebates may be available. Sometimes, installation fees are included in the lease price.

7. ERRORS, DETECTION & CORRECTION

Errors in the data are basically caused due to the various impairments that occur during the process of transmission.When there is an imperfect medium or environment exists in the transmission it prone to errors in the original data.

Transmission errors are usually detected at the physical layer of the OSI model. Transmission errors are usually corrected at the data link layer of the OSI model.

Types of Errors

Single-bit: In a single-bit error, only one bit in the data unit has changed.
Burst :A burst error means that two or more bits in the data unit have changed.

Single-bit error

The change in one bit in the whole data sequence , is called "Single bit error". Occurrence of single bit error is very rare in serial communication system. This type of error

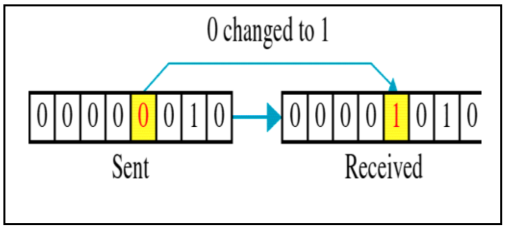


Fig 24 Single bit Error

ccurs only in parallel communication system, as data is transferred bit wise in single line, ere is chance that single line to be noisy.

Burst error

The change of set of bits in data sequence is called “Burst error”. The burst error is calculated in from the first bit change to last bit change.

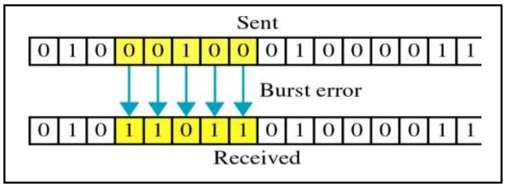


Fig 25 Burst Error

8. Error Detection

Redundancy-is one error detection mechanism. Redundancy is the concept of addition of extrabitstoamessageforerrordetection.Inordertodetectandcorrecttheerrorsinthedata communication we add some extra bits to the original data. These extra bits are nothing but the redundant bits which will be removed by the receiver after receiving the data.

Theirpresenceallowsthereceivertodetectorcorrectcorruptedbits.Insteadofrepeatingthe entire data stream, a short group of bits may be attached to the entire data stream. This technique is called redundancy because the extra bits are redundant to the information: they are discarded as soon as the accuracy of the transmission has been determined.

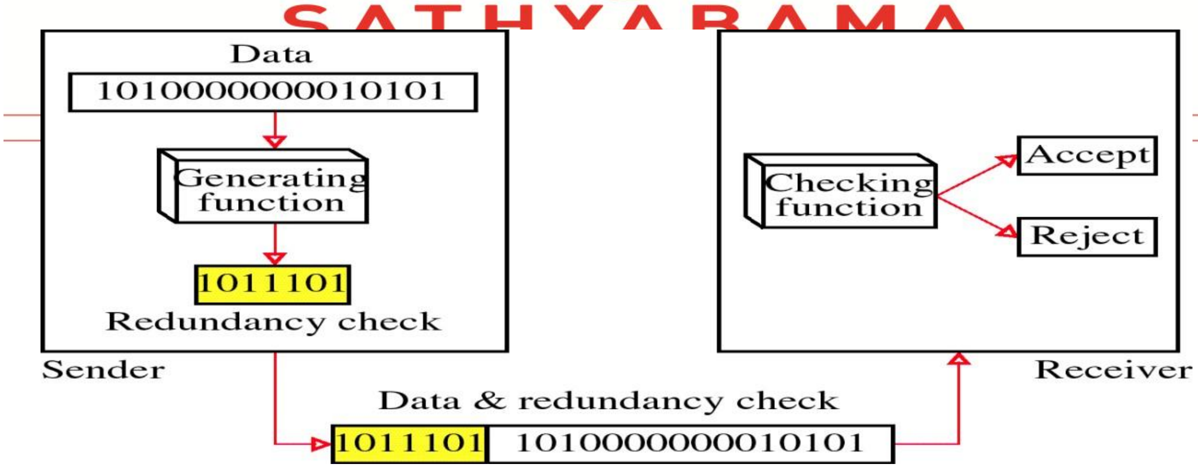


Fig 26 Redundancy

Four types of redundancy checks follows:

a) Vertical redundancy check(VRC)

b) Longitudinal redundancy check(LRC)

c) Cyclic redundancy check(CRC)

d)Checksum

Vertical redundancy check(VRC)

In this technique, a redundant bit ,called a parity bit is added to every data unit so that the total number of 1s becomes even.

Performance: VRC can detect only an odd numbers of errors; it cannot detect an even number of errors.

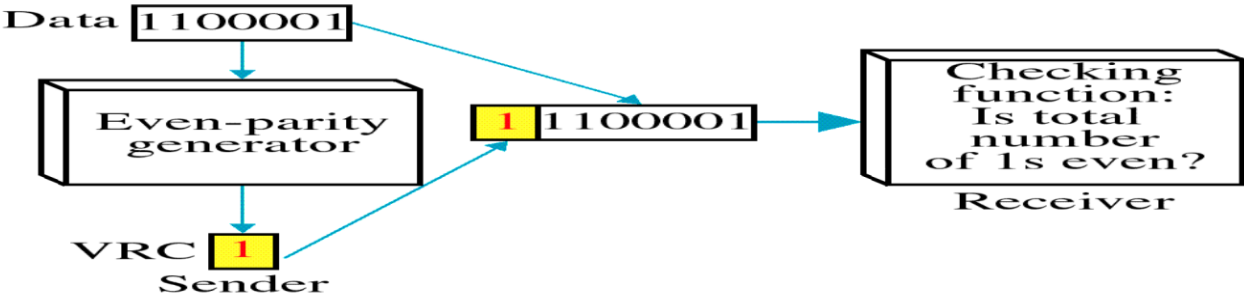


Fig 27 Virtual Redundancy Check

Example: Imagine the sender wants to send the word "world.” In ASCII the five characters are coded as

<--------1110111 1101111 1110010 11011001100100

w o r l d

Each of the first four characters has an even numbers of 1s,so the parity bit is a 0.The last character("d"),however, has three 1s(an odd number),so the parity bit is a 1 to make the total number of 1s even. The following shows the actual bits sent(the parity bits are underlined)

<-------11101110 11011110 11100100 1101100011001001

w o r l d

Example: Now suppose the word "world" in the previous example is received by the receiver but corrupted during transmission.

<------111*1*1110 11011110 1110*1*100 1101100011001001

w o r l d

The receiver counts the 1s in each character and comes up with even and odd numbers(7,6,5,4,4.)The receiver knows that the data are corrupted, discard them, and ask for retransmission.

Longitudinal redundancy check(LRC)

In LRC,a block of bits is organized in a table(rows and columns)

For example, instead of sending a block of 32 bits, we organize them in a table made of four rows and eight columns. We then calculate the parity bit for each column and create a new row of eight bits**.**

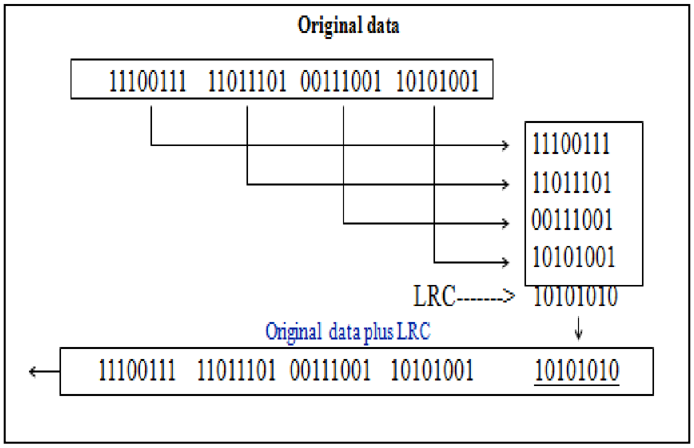


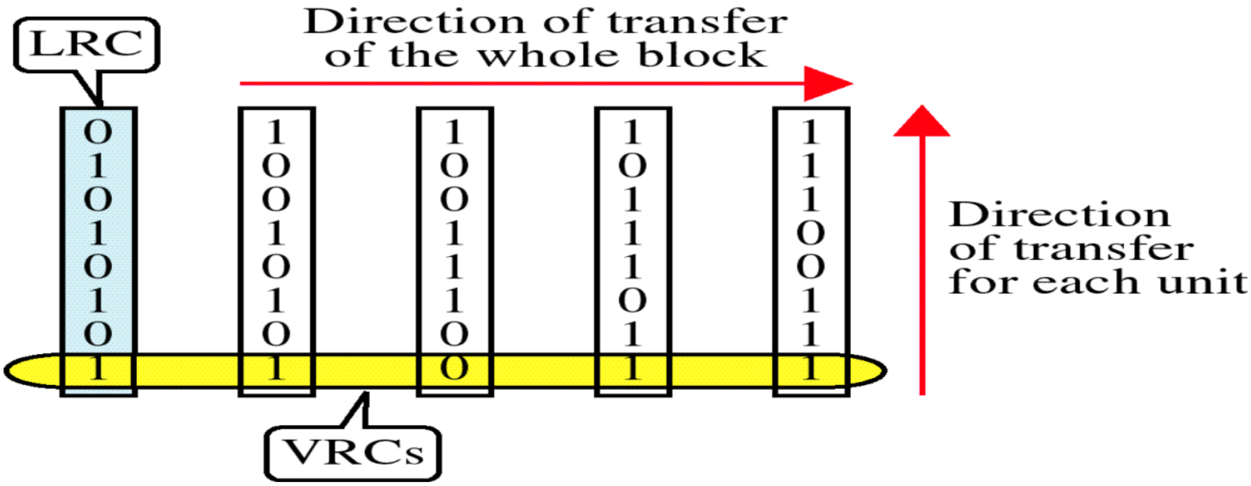
Fig 28 Longitudinal redundancy check

Example: Suppose the following block is sent

<----- 10101001 00111001 11011101 1110011110101010
(LRC)

However, it is hit by a burst noise of length eight and some bits are corrupted.
<----- 1010*001*1 *1000*1001 11011101 1110011110101010
(LRC)

When the receiver checks the LRC,some of the bits do not follow the even-parity rule and the whole block is discarded(the nonmatching bits are shown in bold.
<----- 1010*001*1 *1000*1001 11011101 1110011110101010
(LRC)



CRC and LRC

Fig 29 CRC and LRC

Cyclic redundancy check(CRC)

CRC ,the most powerful of the redundancy checking techniques, is based on binary division. Most powerful of the redundancy checking techniques is the cyclic redundancy check (CRC). This method is based on the binary division. In CRC, the desired sequence of redundant bits are generated and is appended to the end of data unit. It is also called as CRC reminder. So that the resulting data unit becomes exactly divisible by a predetermined binary number.At its destination, the incoming data unit is divided by the same number. If at this step there is no remainder then the data unit indicates that the data unit has been damaged in transit and therefore must be rejected.

The redundancy bits used by CRC are derived by dividing the data unit by a predetermined divisor; the remainder is the CRC.To be valid, a CRC must have two qualities: It must have exactly one less bit than the divisor, and appending it to the end of the data string must make the resulting bit sequence exactly divisible by the divisor.

The following figure shows the process:

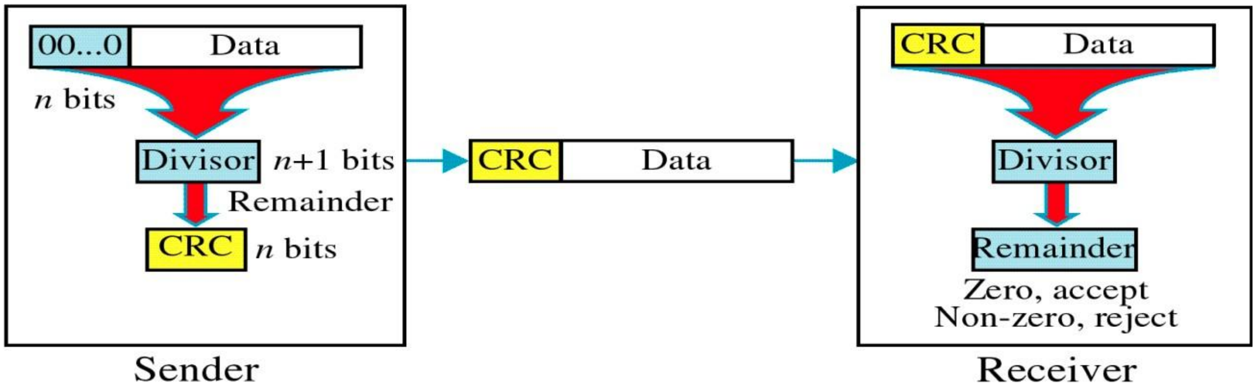


Fig 30 CRC generator and checker

Step1:Astringof0‘sisappendedtothedataunit.Itisnbitslong.Thenumbernis1lessif- number of bits in the predetermined divisor which is n + 1bits.

Step 2: The newly generated data unit is divided by the divisor, using a process called as binary division. The remainder resulting from this division is the CRC.

Step 3: the CRC of n bits derived in step 2 replaces the appended 0‘s at the data unit. Note that the CRC may consist of all 0‘s.

The data unit arrives at the receiver data first, followed by the CRC. The receiver treats the whole string as a unit and divides it by the same divisor that was used the CRC remainder. If the string arrives without error, the CRC checker yields a remainder of zero, the data unit passes. If the string has been changed in transit, the division yields zero remainder and the data unit does not pass.

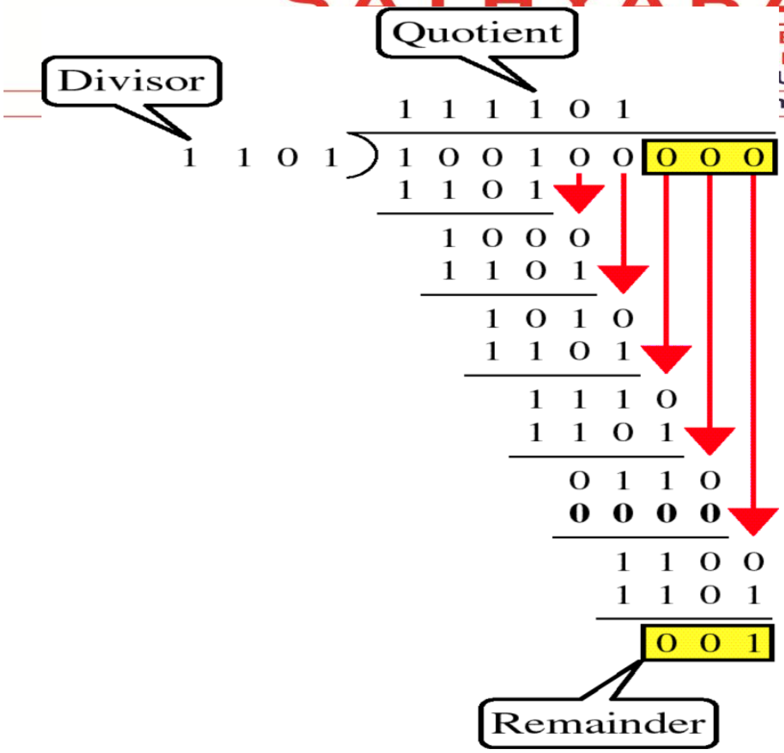


Fig 31 CRC checker Function

A CRC checker functions does exactly as the generator does. After receiving the data appended with the CRC, it does the samemodulo-2 division. If the remainder is all 0‘s, the CRC is dropped and the data is accepted: otherwise, the received stream of bits is discarded and data is resent.

Performance:

CRC is a very effective error detection method. If the divisor is chosen according to the previously mentioned rules,

1. CRC can detect all burst errors that affect an odd number of bits.

2. CRC can detect all burst errors of length less than or equal to the degree of the polynomial

3. CRC can detect, with a very high probability, burst errors of length greater than the degree of the polynomial.

Checksum

A checksum is fixed length data that is the result of performing certain operations on thedata to be sent from sender to the receiver. The sender runs the appropriate checksum algorithm to compute the checksum of the data, appends it as a field in the packet that contains the data to be sent, as well as various headers.

When the receiver receives the data, the receiver runs the same checksum algorithm to compute a fresh checksum. The receiver compares this freshly computed checksum with the checksum that was computed by the sender. If the two checksum matches, the receiver of the data is assured that the data has not changed during the transit. checksum is used by the higher-layer protocols(TCP/IP) for error detection.

To calculate a checksum:

a. Divide the data into sections.
b. Add the sections together using one's complement arithmetic.
c. Take the complement of the final sum; this is the checksum

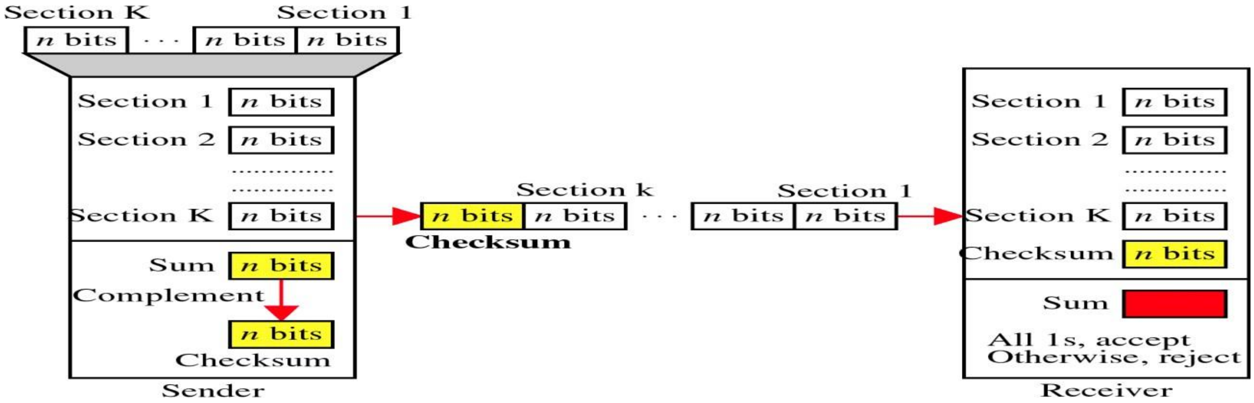


Fig 32 Check Sum

9. Error Correcting Codes

The codes which are used for both error detecting and error correction are called as "Error Correction Codes". The error correction techniques are of two types. They are,

- Single bit error correction
- Burst error correction

The process or method of correcting single bit errors is called "single bit error correction". The method of detecting and correcting burst errors in the data sequence is called "Burst error correction".

Hamming code or Hamming Distance Code is the best error correcting code we use in most of the communication network and digital systems.

Hamming Code

This error detecting and correcting code technique is developed by R.W.Hamming . This code not only identifies the error bit, in the whole data sequence and it also corrects it. This code uses a number of parity bits located at certain positions in the codeword. The number of parity bits depends upon the number of information bits. The hamming code uses the relation between redundancy bits and the data bits and this code can be applied to any number of data bits.

Redundancy Bit

Redundancy means "The difference between number of bits of the actual data sequence and the transmitted bits". These redundancy bits are used in communication system to detect and correct the errors, if any.

Hamming code

In Hamming code, the redundancy bits are placed at certain calculated positions in order to eliminate errors. The distance between the two redundancy bits is called "Hamming distance".

To understand the working and the data error correction and detection mechanism of the hamming code, let's see to the following stages.

Number of parity bits

As we learned earlier, the number of parity bits to be added to a data string depends upon the number of information bits of the data string which is to be transmitted. Number of parity bits will be calculated by using the data bits. This relation is given below.

$2^P >= n + P +1$

Here, n represents the number of bits in the data string.

P represents number of parity bits.

For example, if we have 4 bit data string, i.e. n = 4, then the number of parity bits to be added can be found by using trial and error method. Let's take P = 2, then

$2^P = 2^2 = 4$ and $n + P + 1 = 4 + 2 + 1 = 7$

This violates the actual expression.

So let's try P = 3, then

$2^P = 2^3 = 8$ and $n + P + 1 = 4 + 3 + 1 = 8$

So we can say that 3 parity bits are required to transfer the 4 bit data with single bit error correction.After calculating the number of parity bits required, we should know the appropriate positions to place them in the information string, to provide single bit error correction.In the above considered example, we have 4 data bits and 3 parity bits. So the total codeword to be transmitted is of 7 bits (4 + 3). We generally represent the data sequence from right to left, as shown below.

bit 7, bit 6, bit 5, bit 4, bit 3, bit 2, bit 1, bit 0

The parity bits have to be located at the positions of powers of 2. I.e. at 1, 2, 4, 8 and 16 etc. Therefore the codeword after including the parity bits will be like this

D7, D6, D5, P4, D3, P2, P1

Here P1, P2 and P3 are parity bits. D1 —- D7 are data bits.

Constructing a Bit Location Table

In Hamming code, each parity bit checks and helps in finding the errors in the whole code word. So we must find the value of the parity bits to assign them a bit value. By calculating and inserting the parity bits in to the data bits, we can achieve error correction through Hamming code.

Let's understand this clearly, by looking into an example.

Ex: Encode the data 1101 in even parity, by using Hamming code.

Step 1

Calculate the required number of parity bits.

Let P = 2, then

$2^P = 2^2 = 4$ and $n + P + 1 = 4 + 2 + 1 = 7$.

2 parity bits are not sufficient for 4 bit data.

So let's try P = 3, then

$2^P = 2^3 = 8$ and $n + P + 1 = 4 + 3 + 1 = 8$

Therefore 3 parity bits are sufficient for 4 bit data.

The total bits in the code word are 4 + 3 = 7

Step 2

Constructing bit location table

Step 3

Determine the parity bits.

For P1 : 3, 5 and 7 bits are having three 1's so for even parity, P1 = 1.

For P2 : 3, 6 and 7 bits are having two 1's so for even parity, P2 = 0.
For P3 : 5, 6 and 7 bits are having two 1's so for even parity, P3 = 0.

By entering / inserting the parity bits at their respective positions, codeword can be formed and is transmitted. It is 1100101.

NOTE: If the codeword has all zeros (ex: 0000000), then there is no error in Hamming code.

To represent the binary data in alphabets and numbers, we use alphanumeric codes.

Alpha Numeric Codes

Alphanumeric codes are basically binary codes which are used to represent the alphanumeric data. As these codes represent data by characters, alphanumeric codes are also called "Character codes".

These codes can represent all types of data including alphabets, numbers, punctuation marks and mathematical symbols in the acceptable form by computers. These codes are implemented in I/O devices like key boards, monitors, printers etc.
In earlier days, punch cards are used to represent the alphanumeric codes.

They are

- MORSE code
- BAUDOT code
- HOLLERITH code
- ASCII code
- EBCDI code
- UNICODE

MORSE Code

At the starting stage of computer and digital electronics era, Morse code is very popular and most used code. This was invented by Samuel F.B.Morse, in 1837. It was the first ever telegraphic code used in telecommunication. It is mainly used in Telegraph channels, Radio channels and in air traffic control units.

BOUDOT Code

This code is invented by a French Engineer Emile Baudot, in 1870. It is a 5 unit code, means it uses 5 elements to represent an alphabet. It is also used in Telegraph networks to transfer Roman numeric.

HOLLERITH Code

This code is developed by a company founded by Herman Hollerith in 1896. The 12 bit code used to punch cards according to the transmitting information is called "Hollerith code".

ASCII CODE

ASCII means American Standard Code for Information Interchange. It is the world's most popular and widely used alphanumeric code. This code was developed and first published in 1967. ASCII code is a 7 bit code that means this code uses 27 = 128 characters. This includes

26 lower case letters (a – z), 26 upper case letters (A – Z), 33 special characters and symbols (like ! @ # $ etc), 33 control characters (* – + / and % etc) and 10 digits (0 – 9).

In this 7 bit code we have two parts, the leftmost 3 bits and right side 4 bits. The left most 3 bits are known "ZONE bits" and the right side 4 bits are known as "NUMERIC bits"

Example:

If we want to print the name LONDAN, the ASCII code is?

The ASCII-7 equivalent of L = 100 1100

The ASCII-7 equivalent of O = 100 1111

The ASCII-7 equivalent of N = 100 1110

The ASCII-7 equivalent of D = 100 0100

The ASCII-7 equivalent of A = 100 0001

The ASCII-7 equivalent of N = 100 1110

The output of LONDAN in ASCII code is 1 0 0 1 1 0 0 1 0 0 1 1 1 1 1 0 0 1 1 1 0 1 0 0 0 1 0 0 1 0 0 0 0 0 1 1 0 0 1 1 1 0.

UNICODE

The draw backs in ASCII code and EBCDI code are that they are not compatible to all languages and they do not have sufficient set of characters to represent all types of data. To overcome these drawback this UNICODE is developed. UNICODE is the new concept of all digital coding techniques. In this we have a different character to represent every number. It is the most advanced and sophisticated language with the ability to represent any type of data. SO this is known as "Universal code". It is a 16 bit code, with which we can represent 216 = 65536 different characters. UNICODE is developed by the combined effort of UNICODE consortium and ISO (International organization for Standardization).

EBCDI CODE

EBCDI stands for Extended Binary Coded Decimal Interchange code. This code is developed by IBM Inc Company. It is an 8 bit code, so we can represent 28 = 256 characters by using EBCDI code. This include all the letters and symbols like 26 lower case letters (a – z), 26 upper case letters (A – Z), 33 special characters and symbols (like ! @ # $ etc), 33 control characters (* – + / and % etc) and 10 digits (0 – 9).In the EBCDI code, the 8 bit code the numbers are represented by 8421 BCD code preceded by 1111.

SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

School of Computing

Department of Computer Science and Engineering

UNIT - III

Data Communication and Computer Networks-SBS1302

UNIT III

Multiplexing - types of Multiplexing - Multiplexing Application - Telephone systems project 802 - Ethernet - Token Bus - Token Ring FDD IEEE 802.6 - SMDS - Circuit Switching - Packet switching - Message switching Connection oriented and connectionless services.

1. Multiplexing

Multiplexing is the name given to techniques, which allow more than one message to be transferred via the same communication channel. The channel in this context could be a transmission line, *e.g.* a twisted pair or co-axial cable, a radio system or a fibre optic system *etc*.A channel will offer a specified bandwidth, which is available for a time .

Concept of Multiplexing

Multiplexing is a technique by which different analog and digital streams of transmission can be simultaneously processed over a shared link. Multiplexing divides the high capacity medium into low capacity logical medium which is then shared by different streams.Communication is possible over the air (radio frequency), using a physical media (cable) and light (optical fiber). All mediums are capable of multiplexing.When more than one senders tries to send over single medium, a device called Multiplexer divides the physical channel and allocates one to each. On the other end of communication, a De-multiplexer receives data from a single medium and identifies each and send to different receivers.

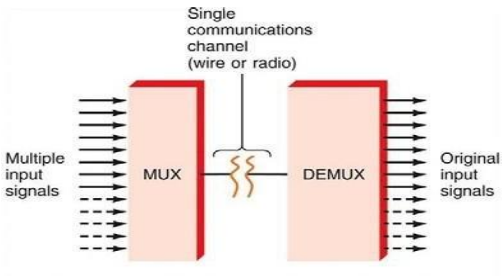


Fig 1 Multiplexing Operation

transmitting two or more signals simultaneously can be accomplished by running multiple cables or setting up one transmitter receiver pair for each channel , but this is an expensive approach. A single cable or radio link can handle multiple signals simultaneously using atechnique known as multiplexing. Multiplexing permits hundreds or even thousands of signals to be combined and transmitted over a single medium.

A device called a multiplexer (often shortened to "mux") combines the input signals into one signal. When the multiplexed signal needs to be separated into its component signal s (for example, when your email is to be delivered to its destination), a device called a demultiplexer (or "demux") isused. Multiplexing was originally developed in the 1800s for telegraphy. Today,multiplexing is widely used in many telecommunications applications, including telephony, Internet communications, digital broadcasting and wireless telephony.

Types of Multiplexing

There are mainly two types of multiplexers, namely analog and digital. They are further divided into Frequency Division Multiplexing (FDM), Wavelength Division Multiplexing (WDM), and Time Division Multiplexing (TDM).

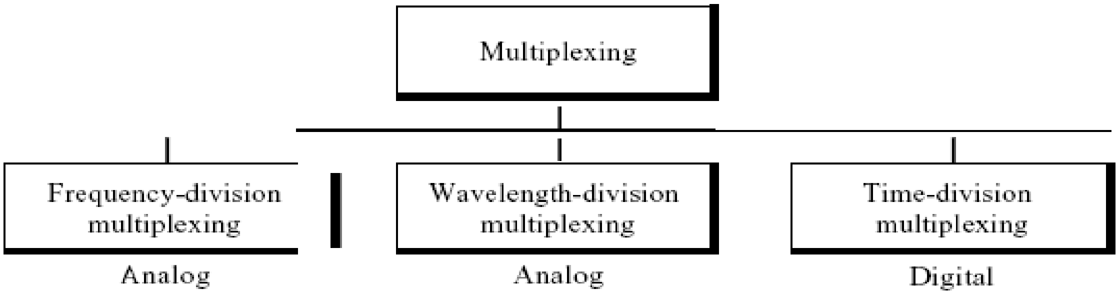

Multiplexing
Frequency-division multiplexing
Wavelength-division multiplexing
Time-division multiplexing
Analog
Analog
Digital

Fig 2 Categories of multiplexing

1) Frequency Division Multiplexing FDM

FDM is derived from AM techniques in which the signals occupy the same physical ‘line’ but in different frequency bands. Each signal occupies its own specific band of frequencies all the time, *i.e*. the messages share the channel **bandwidth**.

2) Time Division MultiplexingTDM

TDM is derived from sampling techniques in which messages occupy all the channel bandwidth but for short time intervals of time, *i.e.* the messages share the channel **time**.TDM – messages occupy **wide** bandwidth – for short intervals of time. Multiplexing is the set of techniques that allows the simultaneous transmission of multiple signals across a single data link.

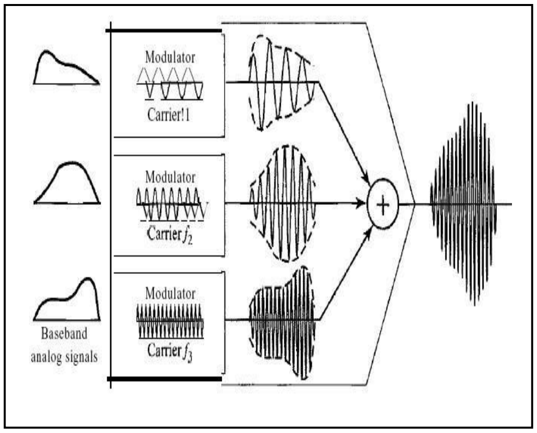


Fig 3 FDM Process

Frequency-Division Multiplexing

Frequency-division multiplexing (FDM) is an analog technique that can be applied when the bandwidth of a link (in hertz) is greater than the combined

bandwidths of the signals to be transmitted. In FOM, signals generated by each sending device modulate different carrier frequencies. These modulated signals are then combined into a single composite signal that can be transported by the link. Carrier frequencies are separated by sufficient bandwidth to accommodate the modulated signal. These bandwidth ranges are the channels through which the various signals travel. Channels can be separated by strips of unused bandwidth-guard bands-to prevent signals from overlapping. In addition, carrier frequencies must not interfere with the original

data frequencies. Fig 4 gives a conceptual view of FDM. In this illustration, the transmission path is divided into three parts, each representing a channel that carries one transmission.

We consider FDM to be an analog multiplexing technique; however, this does not mean that FDM cannot be used to combine sources sending digital signals. A digital signal can be converted to an analog signal before FDM is used to multiplex them.

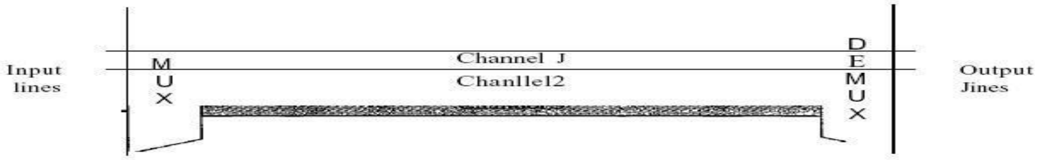


Fig4 FDM

Multiplexing Process

Each source generates a signal of a similar frequency range. Inside the multiplexer, these similar signals modulates different carrier frequencies *(/1,12,* and *h).* The resulting modulated signals are then combined into a single composite signal that is sent out over a media link that has enough bandwidth to accommodate it.

Demultiplexing Process

The demultiplexer uses a series of filters to decompose the multiplexed signal into its constituent component signals. The individual signals are then passed to a demodulator that separates them from their carriers and passes them to the output lines. Fig 5 is a conceptual illustration of demultiplexing process.

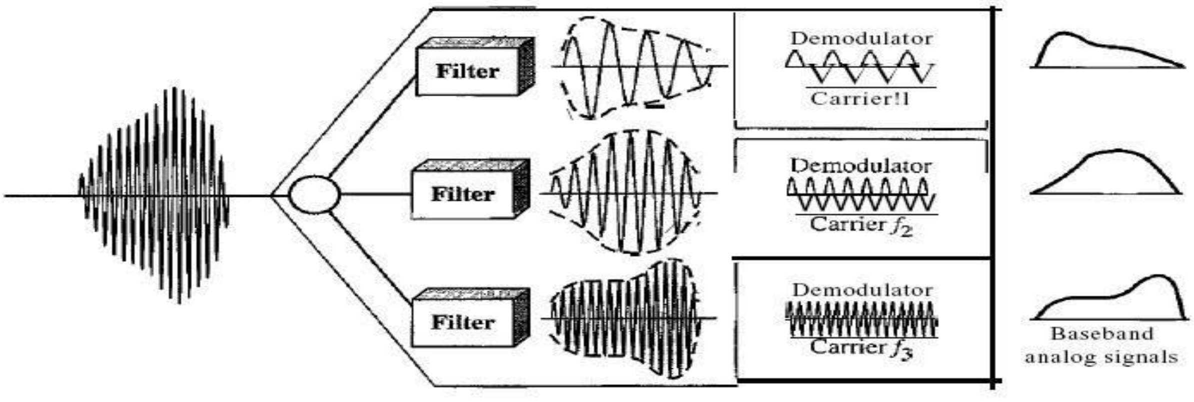


Fig 5 FDM de-multiplexing example

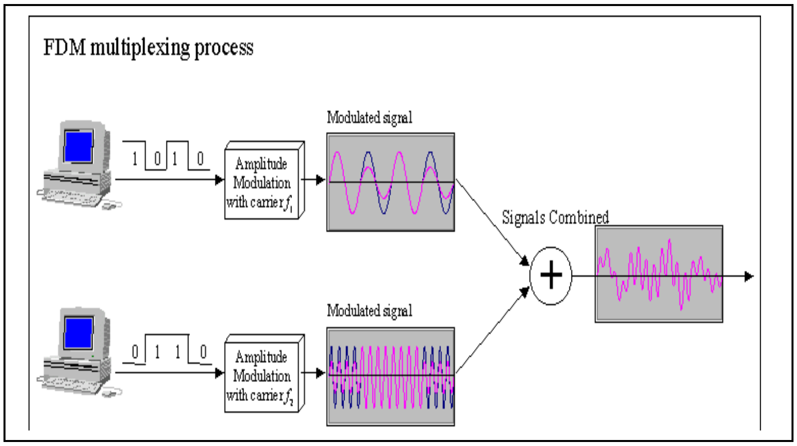


Fig 6 Multiplexing Example

Time Division Multiplexing (TDM): This is possible when data transmission rate of the media is much higher than that of the data rate of the source. Multiple signals can be transmitted ifeach signal is allowed to be transmitted for a definite amount of time. These time slots are so small that all transmissions appear to be in parallel.

Synchronous TDM: Time slots are pre assigned and are fixed. Each source is given it's time slot at every turn due to it. This turn may be once per cycle, or several turns per cycle ,if it has a high data transfer rate, or may be once in a no. of cycles if it is slow. This slot is given even if the source is not ready with data. So this slot is transmitted empty.

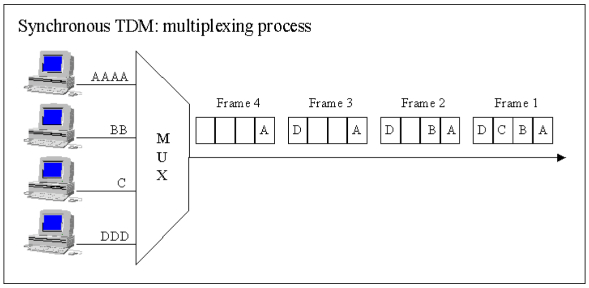


Fig 7

Fig 7 Synchronous TDM

Asynchronous TDM: In this method, slots are not fixed. They are allotted dynamically depending on speed of sources, and whether they are ready for transmission.

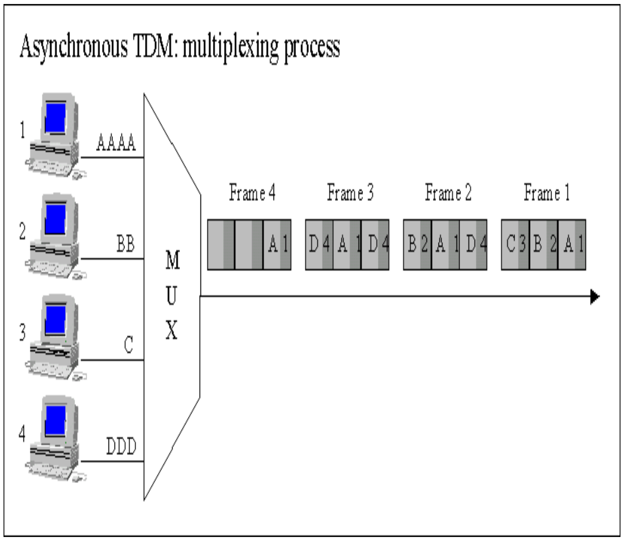


Fig 8Asynchronous TDM

Wavelength-Division Multiplexing

Wavelength-division multiplexing (WDM) is designed to use the high-data-rate capability of fiber-optic cable. The optical fiber data rate is higher than the data rate of metallic transmission cable. Using a fiber-optic cable for one single line wastes the available bandwidth. Multiplexing allows us to combine several lines into one.

WDM is conceptually the same as FDM, except that the multiplexing and demultiplexing involve optical signals transmitted through fiber-optic channels. The idea is the same: We are combining different signals of different frequencies. The difference is that the frequencies are very high.

Fig 9 gives a conceptual view of a WDM multiplexer and demultiplexer. Very narrow bands of light from different sources are combined to make a wider band of light. At the receiver, the signals are separated by the demultiplexer.

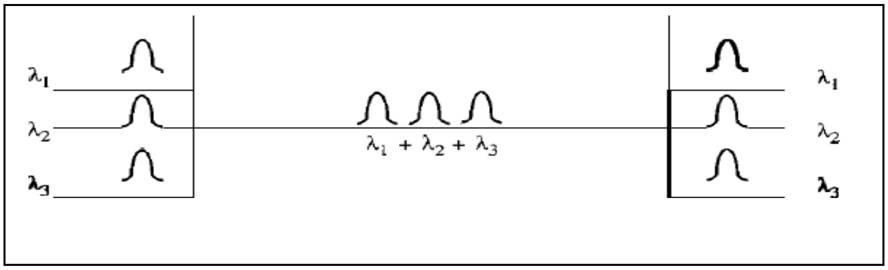


Fig 9Wavelength-division Multiplexing

Although WDM technology is very complex, the basic idea is very simple. We want to combine multiple light sources into one single light at the multiplexer and do the reverse at the demultiplexer. The combining and splitting of light sources are easily handled by a prism. Recall from basic physics that a prism bends a beam of light based on the angle of incidence and the frequency. Using this technique, a multiplexer can be made to combine several input beams of light, each containing a narrow band of frequencies, into one output beam of a wider band of frequencies. A demultiplexer can also be made to reverse the process.

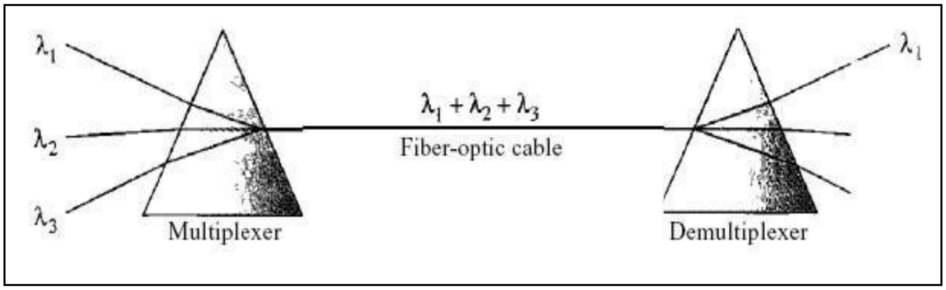


Fig 10 Prisms in wavelength-division multiplexing and demultiplexing

Synchronous Time-Division Multiplexing

Time-division multiplexing (TDM) is a digital process that allows several connections to share the high bandwidth of a linle Instead of sharing a portion of the bandwidth as in FDM, time is shared. Each connection occupies a portion of time in the link. Note that the same link is used as in FDM; here, however, the link is shown sectioned by time rather than by frequency. In the figure, portions of signals 1,2,3, and 4 occupy the link sequentially.

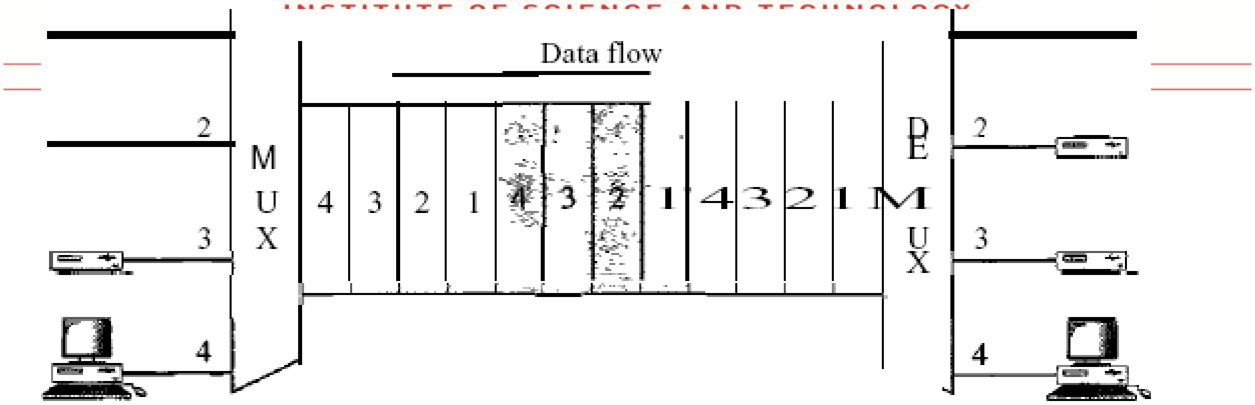


Fig 11 TDM

All the data in a message from source 1 always go to one specific destination, be it 1, 2, 3, or 4. The delivery is fixed and unvarying, unlike switching. We also need to remember thatTDM is, in principle, a digital multiplexing technique. Digital data from different sources are combined into one timeshared link. However, this does not mean that the sources cannot produce analog data; analog data can be sampled, changed to digital data, and then multiplexed by using TDM.

We can divide TDM into two different schemes: synchronous and statistical.

In synchronous TDM, each input connection has an allotment in the output even if it is not sending data.

Time Slots and Frames

In synchronous TDM, the data flow of each input connection is divided into units, where each input occupies one input time slot. A unit can be 1 bit, one character, or one block of data. Each input unit becomes one output unit and occupies one output time slot. However, the duration of an output time slot is *n* times shorter than the duration of an input time slot. If an input time slot is *T* s,the output time slot is*Tin*s,where *n* is the number of connections.Inotherwords,aunitin the ut connection has a shorter duration; it travels faster. Figure shows an example of synchronous TDM where *n* is 3.

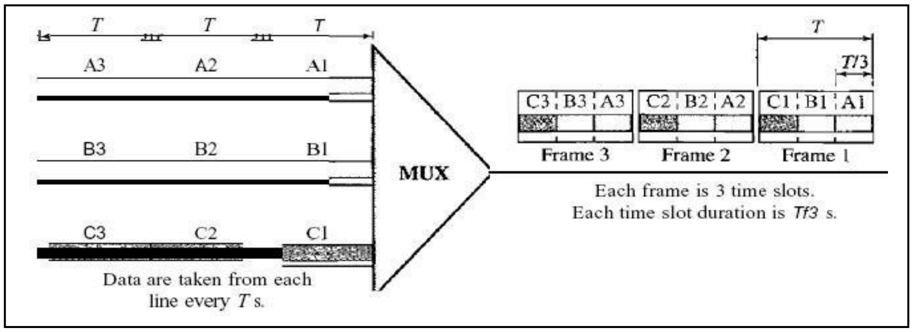

T
T
T
A3
A2
A1
B3
B2
B1
C3
C2
C1
MUX
Data are taken from each line every T s.
T
T/3
C3 B3 A3
C2 B2 A2
C1 B1 A1
Frame 3
Frame 2
Frame 1
Each frame is 3 time slots.
Each time slot duration is Tf3 s.

Fig 12 ***Synchronous time-division multiplexing***

In synchronous TDM, a round of data units from each input connection is collected into a frame (we will see the reason for this shortly). If we have *n* connections, a frame is divided into *n* time slots and one slot is allocated for each unit, one for each input line. If the duration of the input unit is *T*, the duration of each slot is *Tin* and the duration of each frame is *T* (unless a frame carries some other information, as we will see shortly).

The data rate of the output link must be *n* times the data rate of a connection to guarantee the flow of data. In Figure 7, the data rate of the link is 3 times the data rate of a connection; likewise, the duration of a unit on a connection is 3 times that of the time slot (duration of a unit on the link). In the figure we represent the data prior to multiplexing as 3 times the size of the data after multiplexing. This is just to convey the idea that each unit is 3 times longer in duration before multiplexing than after. Time slots are grouped into frames. A frame consists of one complete cycle of time slots, with one slot dedicated to each sending device. In a system with *n* input lines, each frame has *n* slots, with each slot allocated to carrying data from a specific input line.

Interleaving

TDM can be visualized as two fast-rotating switches, one on the multiplexing side and the other on the demultiplexing side. The switches are synchronized and rotate at the same speed, but in opposite directions. On the multiplexing side, as the switch opens in front of a connection,thatconnection has the opportunity to send a unit onto the path. This process is called **interleaving.** On the demultiplexing side, as the switch opens in front of a connection, that connection has the opportunity to receive a unit from thepath.

In this figure, we assume that no switching is involved and that the data from the first connection at the multiplexer site go to the first connection at the demultiplexer

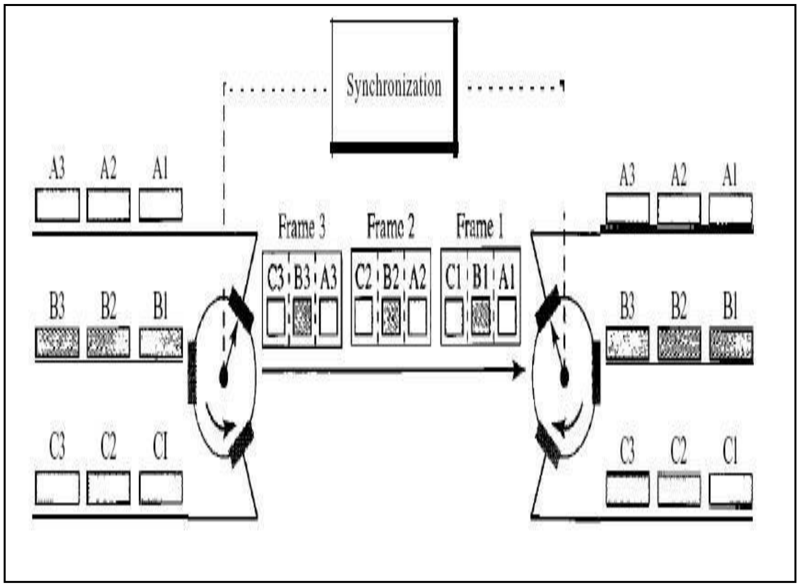


Fig 13 Interleaving

Statistical Time-Division Multiplexing

Addressing

Figure a also shows a major difference between slots in synchronous TDM and statistical TDM. An output slot in synchronous TDM is totally occupied by data; in statistical TDM, a slot needs to carry data as well as the address of the destination.

In synchronous TDM, there is no need for addressing; synchronization and preassigned relationships between the inputs and outputs serve as an address. We know, for example, that input 1 always goes to input 2. If the multiplexer and the demultiplexer are synchronized, this is guaranteed. In statistical multiplexing, there is no fixed relationship between the inputs and outputs because there are no pre assigned or reserved slots. We need to include the address of the receiver inside each slot to show where it is to be delivered. The addressing in its simplest form can be *n* bits to define *N* different output lines with *n* =10g2 *N*. For example, for eight different output lines, we need a 3-bitaddress.

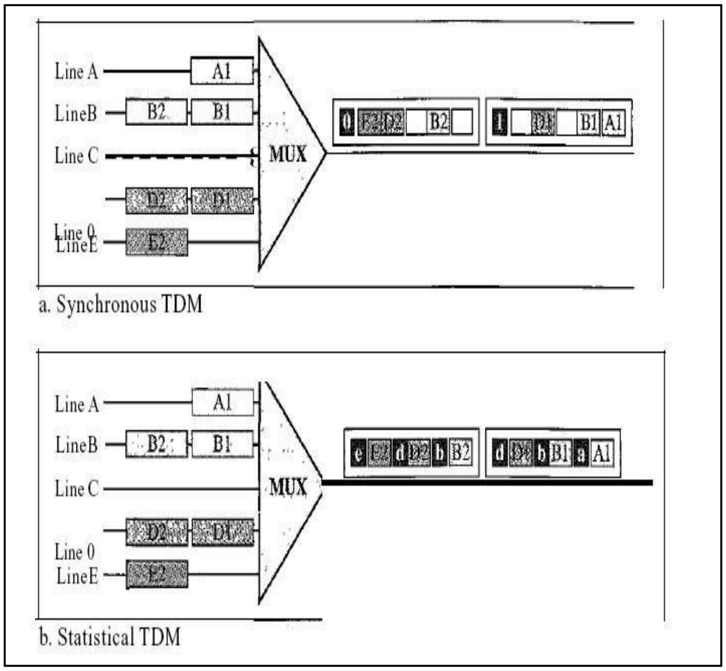


Fig 14 TDM slot comparison

Slot Size

Since a slot carries both data and an address in statistical TDM, the ratio of the data size to address size must be reasonable to make transmission efficient. For example, it would be inefficient to send 1 bit per slot as data when the address is 3 bits. This would mean an overhead of 300 percent. In statistical TDM, a block of data is usually many bytes while the address is just a few bytes.

No Synchronization Bit

There is another difference between synchronous and statistical TDM, but this time it is at the frame level. The frames in statistical TDM need not be synchronized, so we do not need synchronization bits.

Bandwidth

In statistical TDM, the capacity of the link is normally less than the sum of the capacities of each channel. The designers of statistical TDM define the capacity of the link based on the statistics of the load for each channel. If on average only *x* percent of the input slots are filled, the capacity of the link reflects this. Of course, during peak times, some slots need to wait.

2. Applications of Multiplexers

A Multiplexer is used in numerous applications like, where multiple data can be transmitted using a single line.

Communication System – A Multiplexer is used in communication systems, which has a transmission system and also a communication network. A Multiplexer is used to increase the efficiency of the communication system by allowing the transmission of data such as audio & video data from different channels via cables and single lines.

Computer Memory – A Multiplexer is used in computer memory to keep up a vast amount of memory in the computers, and also to decrease the number of copper lines necessary to connect the memory to other parts of the computer.

Telephone Network – A multiplexer is used in telephone networks to integrate the multiple audio signals on a single line of transmission. In a telephone network, the multiple audio signals are brought into a single line and transmitted with the implementation of a Mux. By this way, the numerous audio signals are made isolated and ultimately the recipient will receive the required audio signals.

Computer System of a Satellite Transmission- Mux is used for the data signals to be transmitted from spacecraft or computer system of a satellite to the earth by means of GPS.

3. IEEE Standards

The IEEE has subdivided the data link layer into two sublayers: logical link control (LLC) and media access control (MAC). IEEE has also created several physical layer standards for different LAN protocols.

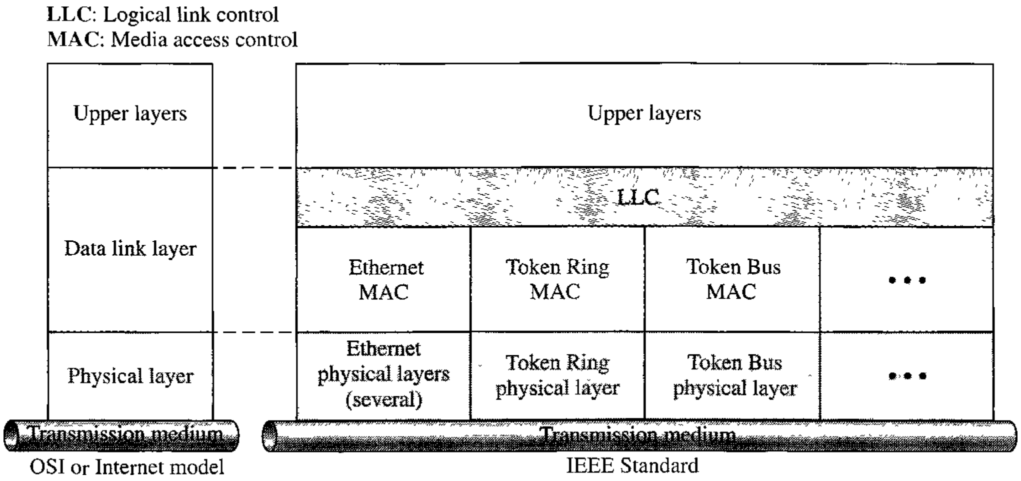


Fig 15 IEEE Standards

Data Link Layer

The data link layer in the IEEE standard is divided into two sublayers: LLC and MAC.

Logical Link Control (LLC)

In IEEE Project 802, flow control, error control, and part of the framing duties are collected into one sublayer called the logical link control. Framing is handled in both the LLC sublayer and the MAC sublayer.

The LLC provides one single data link control protocol for all IEEE LANs. In this way, the LLC is different from the media access control sublayer, which provides different protocols for different LANs. A single LLC protocol can provide interconnectivity between different LANs because it makes the MAC sublayer transparent.

Framing LLC defines a protocol data unit (PDU) that is somewhat similar to that of HDLC. The header contains a control field like the one in HDLC; this field is used for flow and error control. The two other header fields define the upper-layer protocol at the source and destination that uses LLC. These fields are called the destination service access point (DSAP) and the source service access point (SSAP). The other fields defined in a typical data link control protocol such as HDLC are moved to the MAC sublayer. In other words, a frame defined in HDLC is divided into a PDU at the LLC sublayer and a frame at the MAC sublayer, as shown in figure.

Need for LLC The purpose of the LLC is to provide flow and error control for the upper-layer protocols that actually demand these services. For example, if a LAN or several LANs are used in an isolated system, LLC may be needed to provide flow and error control for the application layer protocols. However, most upper-layer protocols such as IP, do not use the services of LLC.

Media Access Control (MAC)

IEEE Project 802 has created a sub layer called media access control that defines the specific access method for each LAN. For example, it defines CSMA/CD as the media access method for Ethernet LANs and the token-passing method for Token Ring and Token Bus LANs. Part of the framing function is also handled by the MAC layer.In contrast to the LLC sublayer, the MAC sublayer contains a number of distinct modules; each defines the access method and the framing format specific to the corresponding LAN protocol.

Physical Layer

The physical layer is dependent on the implementation and type of physical media used. IEEE defines detailed specifications for each LAN implementation. For example, although there is only one MAC sublayer for Standard Ethernet, there is a different physical layer specification for each Ethernet implementations.

Key features of LANs are summarized below:

- Limited geographical area – which is usually less than 10 Km and more than 1m.
- High Speed – 10 Mbps to 1000 Mbps (1 Gbps) and more
- High Reliability – 1 bit error in 10^{11}bits.
- Transmission Media – Guided and unguided media, mainly guided media is used; except in a situation where infrared is used to make a wireless LAN in a room.
- Topology – It refers to the ways in which the nodes are connected. There are various topologies used.

Medium-Access Control Techniques –Some access control mechanism is needed to decide which station will use the shared medium at a particular point in time.

For the fulfillment of the abovementioned goals, the committee came up with a bunch of LAN standards collectively known as IEEE 802 LANs. To satisfy diverse requirements, the standard includes CSMA/CD, Token bus, Token

Ring medium access control techniques along with different topologies. All these standards differ at the physical layer and MAC sublayer, but are compatible at the data link layer.

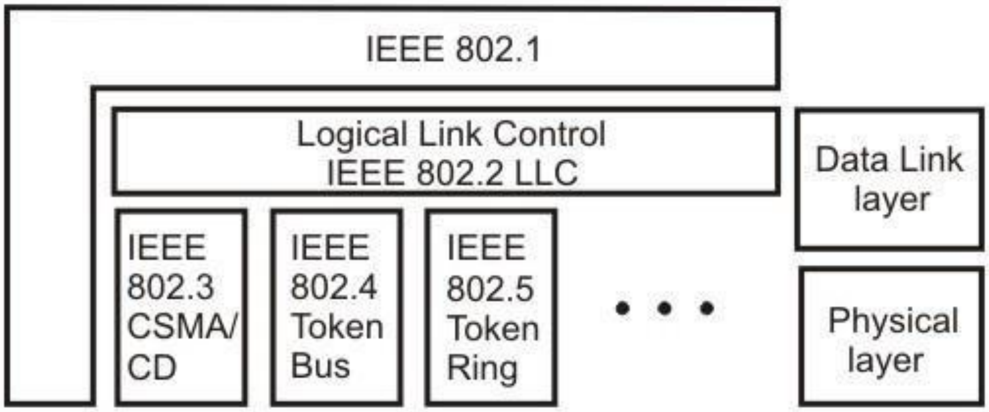


Fig 16 IEEE 802 Legacy LANs

The **802.1** sublayer gives an introduction to set of standards and gives the details of the interface primitives. It provides relationship between the OSI model and the 802 standards. The **802.2** sublayer describes the **LLC** (logical link layer), which is the upper part of the data link layer. LLC facilitate error control and flow control for reliable communication. It appends a header containing sequence number and acknowledgement number. And offers the following three types of services:

- Unreliable datagram service
- Acknowledged datagram service
- Reliable connection oriental service

The standards 802.3, 802.4 and 802.5 describe three LAN standards based on the CSMA/CD, token bus and token ring, respectively. Each standard covers the physical layer and MAC sublayer protocols. In the following sections we shall focus on these three LAN standards.

4. IEEE 802.3 and Ethernet

Ethernet - A Brief History

The original Ethernet was developed as an experimental coaxial cable network in the 1970s by Xerox Corporation to operate with a data rate of 3 Mbps using a carrier sense multiple access collision detection (CSMA/CD) protocol for LANs with sporadic traffic requirements. Success with that project attracted early attention and led to the 1980 joint development of the 10-Mbps Ethernet Version 1.0 specification by the three-company consortium: Digital Equipment Corporation, Intel Corporation, and Xerox Corporation.

The original IEEE 802.3 standard was based on, and was very similar to, the Ethernet Version 1.0 specification. The draft standard was approved by the 802.3 working group in 1983 and was subsequently published as an official standard in 1985 (ANSI/IEEEStd.

802.3-1985). From then onwards, the term *Ethernet* refers to the family of local-area network (LAN) products covered by the IEEE 802.3 standard that defines what is commonly known as the CSMA/CD protocol. Three data rates are currently defined for operation over optical fiber and twisted-pair cables:

- 10 Mbps—10Base-TEthernet
- 100 Mbps—FastEthernet
- 1000 Mbps—GigabitEthernet

Ethernet has survived as the major LAN technology (it is currently used for approximately 85 percent of the world's LAN-connected PCs and workstations) because its protocol has the following characteristics:

- It is easy to understand, implement, manage, and maintain It allows low-cost network implementations
- It provides extensive topological flexibility for network installation
- It guarantees successful interconnection and operation of standards-compliant products, regardless of manufacturer

Ethernet Architecture

Ethernet architecture can be divided into two layers:

- **Physical layer:** this layer takes care of following functions.
- Encoding and decoding
- Collision detection
- Carrier sensing
- Transmission and receipt
- **Data link layer:** Following are the major functions of this layer.
- Station interface

- Data Encapsulation/De capsulation
- Link management
- Collision Management

STANDARD ETHERNET

The original Ethernet was created in 1976 at Xerox's Palo Alto Research Center (PARC). Since then, it has gone through four generations: Standard Ethernet (10 t Mbps), Fast Ethernet (100 Mbps), Gigabit Ethernet (1 Gbps), and Ten-Gigabit Ethernet (10 Gbps), as shown in the figure:

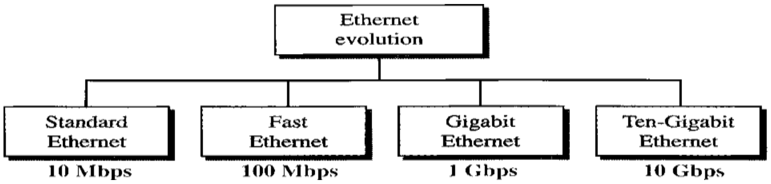


Fig 17 Types of Ethernet

MAC Sublayer

In Standard Ethernet, the MAC sub layer governs the operation of the access method. It also frames data received from the upper layer and passes them to the physical layer.

Frame Format

The Ethernet frame contains seven fields: preamble, SFD, DA, SA, length or type of protocol data unit (PDU), upper-layer data, and the CRC. Ethernet does not provide any mechanism for acknowledging received frames, making it what is known as an unreliable medium. Acknowledgments must be implemented at the higher layers. The format of the MAC frame is shown in the figure.

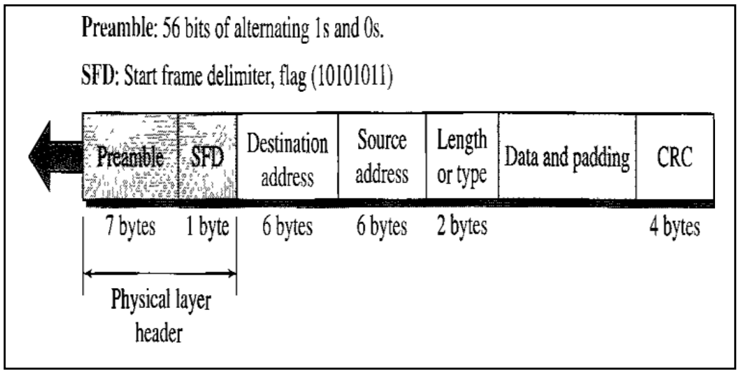


Fig 18 a) MAC Frame

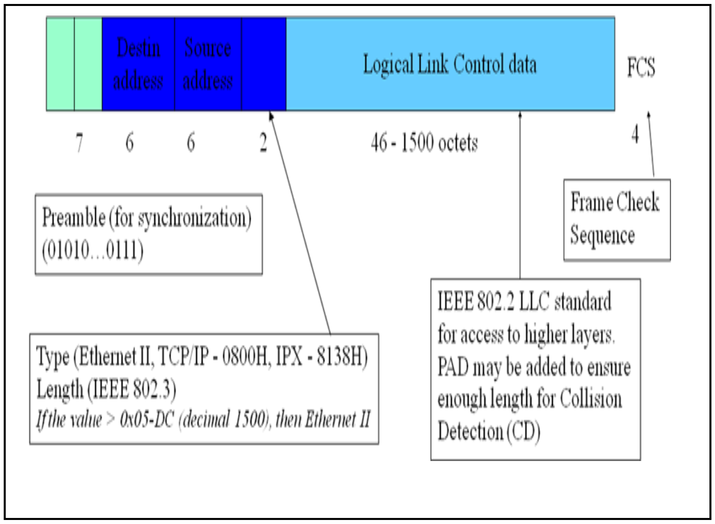

Destn address
Source address
Logical Link Control data
FCS
7
6
6
2
46 - 1500 octets
4
Preamble (for synchronization) (01010…0111)
Frame Check Sequence
IEEE 802.2 LLC standard for access to higher layers. PAD may be added to ensure enough length for Collision Detection (CD)
Type (Ethernet II, TCP/IP - 0800H, IPX - 8138H) Length (IEEE 802.3)
If the value > 0x05-DC (decimal 1500), then Ethernet II

Fig 18 b) MAC Frame Description

- **Preamble**. The first field of the 802.3 frame contains 7 bytes (56 bits) of alternating 0s and 1s that alerts the receiving system to the coming frame and enables it to synchronize its input timing. The pattern provides only an alert and a timing pulse. The 56-bit pattern allows the stations to miss some bits at the beginning of the frame. The preamble is actually added at the physical layer and is not (formally) part of the frame.
- **Start frame delimiter (SFD).** The second field (1 byte: 10101011) signals the beginning of the frame. The SFD warns the station or stations that this is the last chance for synchronization. The last 2 bits is 11 and alerts the receiver that the next field is the destination address.
- **Destination address (DA)**. The DA field is 6 bytes and contains the physical address of the destination station or stations to receive the packet.
- **Source address (SA)**. The SA field is also 6 bytes and contains the physical address of the sender of the packet.
- **Length or type**. This field is defined as a type field or length field. The original Ethernet used this field as the type field to define the upper-layer protocol using the MAC frame. The IEEE standard used it as the length field to define the number of bytes in the data field.
- **Data**. This field carries data encapsulated from the upper-layer protocols. It is a minimum of 46 and a maximum of 1500bytes.

- **CRC**. The last field contains error detection information, in this case aCRC-32.

Frame Length

Ethernet has imposed restrictions on both the minimum and maximum lengths of a frame, as shown in figure.

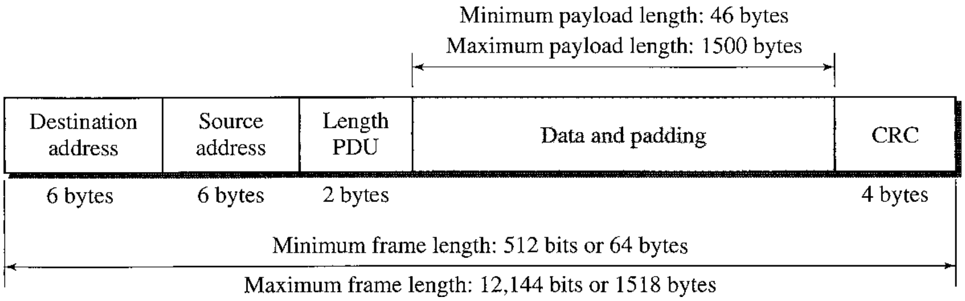

Minimum payload length: 46 bytes
Maximum payload length: 1500 bytes
Destination address
Source address
Length PDU
Data and padding
CRC
6 bytes
6 bytes
2 bytes
4 bytes
Minimum frame length: 512 bits or 64 bytes
Maximum frame length: 12,144 bits or 1518 bytes

Fig 19 Frame Length

The minimum length restriction is required for the correct operation of CSMA/CD. An Ethernet frame needs to have a minimum length of 512 bits or 64 bytes. Part of this length is the header and the trailer. If we count 18 bytes of header and trailer (6 bytes of source address, 6 bytes of destination address, 2 bytes of length or type, and 4 bytes of CRC), then the minimum length of data from the upper layer is 64 - 18 = 46 bytes. If the upper-layer packet is less than 46 bytes, padding is added to make up the difference.

The standard defines the maximum length of a frame (without preamble and SFD field) as 1518 bytes. If we subtract the 18 bytes of header and trailer, the maximum length of the payload is 1500 bytes. The maximum length restriction has two historical reasons. First, memory was very expensive when Ethernet was designed: a maximum length restriction helped to reduce the size of the buffer. Second, the maximum length restriction prevents one station from monopolizing the shared medium, blocking other stations that have data to send.

Addressing

Each station on an Ethernet network (such as a PC, workstation, or printer) has its own network interface card (NIC). The NIC fits inside the station and provides the station with a 6-byte physical address. As shown in the figure, the Ethernet address is 6 bytes (48 bits), normally written in hexadecimal notation, with a colon between the bytes.

Unicast, Multicast, and Broadcast Addresses A source address is always a unicast address--the frame comes from only one station. The destination address, however, can be unicast, multicast, or broadcast. The following figure shows how to distinguish a unicast address from a multicast address. If the least significant bit of the first byte in a destination address is 0, the address is unicast; otherwise, it is multicast.

A unicast destination address defines only one recipient; the relationship between the sender and the receiver is one-to-one. A multicast destination address defines a group of addresses; the relationship between the sender and the receivers is one4o-many. The broadcast address is a special case of the multicast address; the recipients are all the stations on the LAN. A broadcast destination address is forty-eight ls.

Access Method: CSMA/CD

Standard Ethernet uses 1-persistent CSMA/CD

Slot Time In an Ethernet network, the round-trip time required for a frame to travel from one end of a maximum-length network to the other plus the time needed to send the jam sequence is called the slot time.

Slot time = round-trip time + time required to send the jam sequence

The slot time in Ethernet is defined in bits. It is the time required for a station to send 512 bits. This means that the actual slot time depends on the data rate; for traditional 10- Mbps Ethernet it is51.2μs.

Slot Time and Collision The choice of a 512-bit slot time was not accidental. It Waschosen to allow the proper functioning of CSMA/CD. To understand the situation, let us consider two cases.

In the first case, we assume that the sender sends a minimum-size packet of 512 bits. Before the sender can send the entire packet out, the signal travels through the network and reaches the end of the network. If there is another signal at the end of the network (worst case), a collision occurs. The sender has the opportunity to abort the sending of the frame and to send a jam sequence to inform other stations of the collision. The roundtrip time plus the time required to send the jam sequence should be less than the time needed for the sender to send the minimum frame, 512 bits. The sender needs to be aware of the collision before it is too late, that is, before it has sent the entire frame.

In the second case, the sender sends a frame larger than the minimum size (between 512 and 1518 bits). In this case, if the station has sent out the first 512 bits and has not hearda collision, it is guaranteed that collision will never occur during the transmission of this frame. The reason is that the signal will reach the end of the network in less than one- half the slot time. If all stations follow the CSMA/CD protocol, they have already sensed the existence of the signal (carrier) on the line and have refrained from sending. If they sent a signal on the line before one- half of the slot time expired, a collision has occurred and the sender has sensed the collision. In other words, collision can only occur during the first half of the slot time, and if it does, it can be sensed by the sender during the slot time. This means that after the sender sends the first 512 bits, it is guaranteed that collision will not occur during the transmission of this frame. The medium belongs to the sender, and no other station will use it. In other words, the sender needs to listen for a collision only during the time the first 512 bits aresent.

Slot Time and Maximum Network Length There is a relationship between the slot time and the maximum length of the network (collision domain). It is dependent on the propagation speed of the signal in the particular medium. In most transmission media, the signal propagates at 2 x 108 m/s (two-thirds of the rate for propagation in air). For traditional Ethernet, wecalculate

$$\text{MaxLength} = \text{PropagationSpeed} \times \frac{\text{SlotTime}}{2}$$

$$\text{MaxLength} = (2 \times 10^{8}) \times (51.2 \times 10^{-6} / 2) = 5120 \text{ m}$$

Of course, we need to consider the delay times in repeaters and interfaces, and the time required to send the jam sequence. These reduce the maximum-length of a traditional Ethernet network to 2500 m, just 48 percent of the theoretical calculation.

MaxLength = 2500 m

Physical Layer

The Standard Ethernet defines several physical layer implementations; four of the most common, are shown in figure.

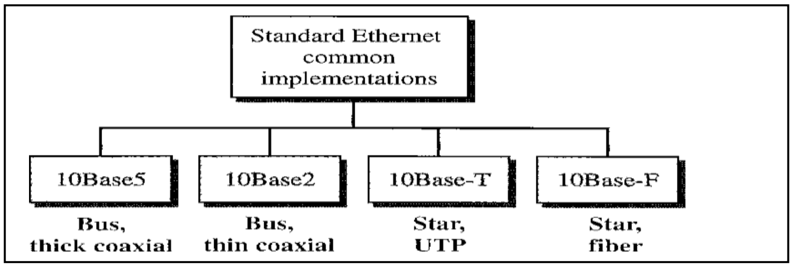


Fig 20 Ethernet Description

Because Ethernet devices implement only the bottom two layers of the OSI protocol stack, they are typically implemented as network interface cards (NICs) that plug into the host device's motherboard, or presently built-in in the motherboard. The naming convention is a concatenation of three terms indicating the transmission rate, the transmission method, and the media type/signal encoding. Consider for example, 10Base-T. where 10 implies transmission rate of 10 Mbps, Base represents that it uses baseband signaling, andTrefers to twisted-pair cables as transmission media. Various standards are discussed below:

Encoding and Decoding

All standard implementations use digital signaling (baseband) at 10 Mbps. At the sender, data are converted to a digital signal using the Manchester scheme; at the receiver, the received signal is interpreted as Manchester and decoded into data. The figure shows the encoding scheme for StandardEthernet.

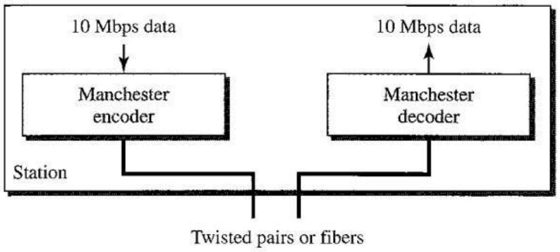


Fig 21 Encoding Scheme

10Base5: Thick Ethernet

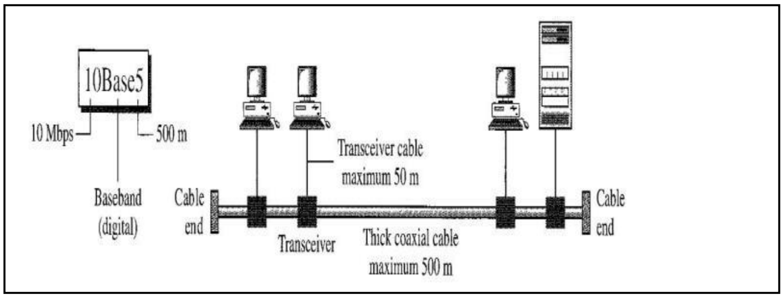
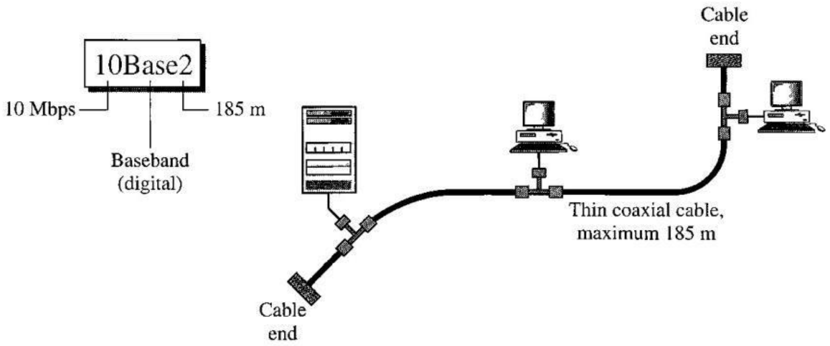


Fig 22 Thick Ethernet

10Base5 was the first Ethernet specification to use a bus topology with an external transceiver (transmitter/receiver) connected via a tap to a thick coaxial cable. The transceiver is responsible for transmitting, receiving, and detecting collisions.

The transceiver is connected to the station via a transceiver cable that provides separate paths for sending and receiving. This means that collision can only happen in the coaxial cable.

The maximum length of the coaxial cable must not exceed 500 m, otherwise, there is excessive degradation of the signal. If a length of more than 500 m is needed, up to five segments, each a maximum of 500-meter, can be connected using repeaters.



10Base2: Thin Ethernet

Fig 23 Thin Ethernet

10Base2 also uses a bus topology, but the cable is much thinner and more flexible. The cable can be bent to pass very close to the stations. In this case, the transceiver is normally part of the network interface card (NIC), which is installed inside the station.

Note that the collision here occurs in the thin coaxial cable. This implementation is more cost effective than 10Base5 because thin coaxial cable is less expensive than thick coaxial and the tee connections are much cheaper than taps. Installation is simpler because the thin coaxial cable is very flexible. However, the length of each segment cannot exceed 185 m (close to 200 m) due to the high level of attenuation in thin coaxial cable.

10Base- T: Twisted-Pair Ethernet

The third implementation is called 10Base-T or twisted-pair Ethernet. 10Base-T uses a physical star topology. The stations are connected to a hub via two pairs of twisted cable.

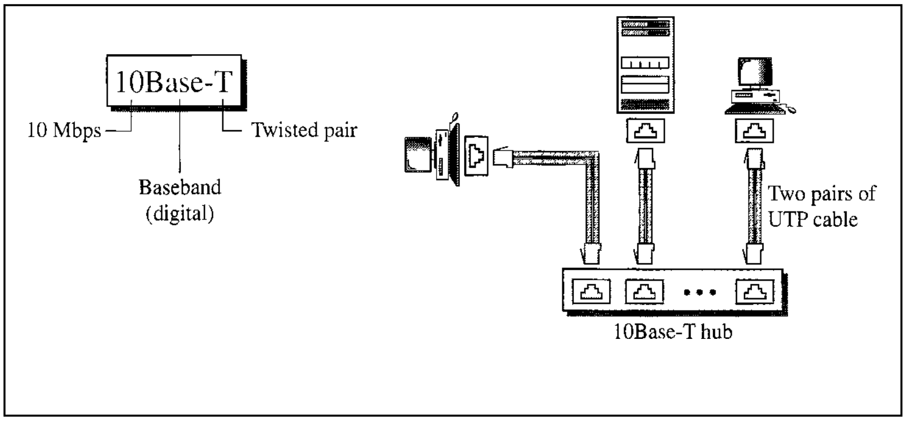


Fig 24 Twisted Pair

Note that two pairs of twisted cable create two paths (one for sending and one for receiving) between the station and the hub. Any collision here happens in the hub. Compared to 10Base5 or 10Base2, we can see that the hub actually replaces the coaxial cable as far as a collision is concerned. The maximum length of the twisted cable here is defined as 100 m, to minimize the effect of attenuation in the twisted cable.

10Base-F: Fiber Ethernet

10Base-F uses a star topology to connect stations to a hub. The stations are connected to the hub using two fiber-optic cables.

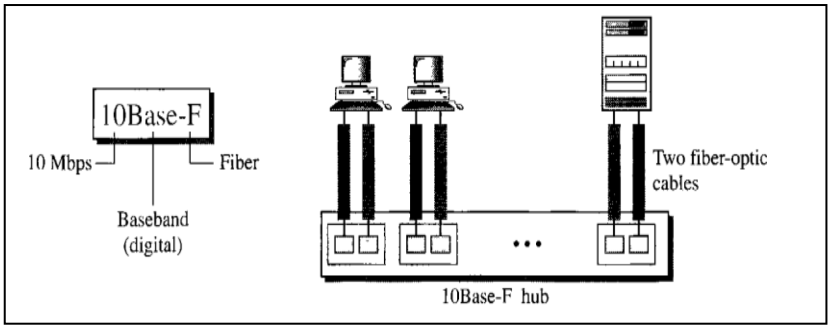


Fig 25 Fiber Ethernet

No Need for CSMA/CD

In full-duplex switched Ethernet, there is no need for the CSMA/CD method. In a full-duplex switched Ethernet, each station is connected to the switch via two separate links. Each station or switch can send and receive independently without worrying about collision. Each link is a point-to-point dedicated path between the station and the switch. There is no longer a need for carrier sensing; there is no longer a need for collision detection. The job of the MAC layer becomes much easier. The carrier sensing and collision detection functionalities of the MAC sub layer can be turned off.

MAC Control Layer

Standard Ethernet was designed as a connectionless protocol at the MAC sublayer. There is no explicit flow control or error control to inform the sender that the frame has arrived at the destination without error. When the receiver receives the frame, it does not send any positive or negative acknowledgment.
To provide for flow and error control in full-duplex switched Ethernet, a new sublayer, called the MAC control, is added between the LLC sublayer and the MAC sublayer.

FAST ETHERNET

Fast Ethernet was designed to compete with LAN protocols such as FDDI or Fiber Channel (or Fibre Channel, as it is sometimes spelled). IEEE created Fast Ethernet under the name 802.3u. Fast Ethernet is backward-compatible with Standard Ethernet, but it can transmit data 10 times faster at a rate of 100 Mbps. The goals of Fast Ethernet can be summarized as follows:

1. Upgrade the data rate to 100Mbps.
2. Make it compatible with Standard Ethernet.
3. Keep the same 48-bitaddress.
4. Keep the same frame format.
5. Keep the same minimum and maximum frame lengths.

MAC Sub layer

A main consideration in the evolution of Ethernet from 10 to 100 Mbps was to keep the MAC sub layer untouched. However, a decision was made to drop the bus topologies and keep only the star topology. For the star topology, there are two choices, as we saw before: half duplex and full duplex. In the half-duplex approach, the stations are connected via a hub; in the full- duplex approach, the connection is made via a switch with buffers at each port.
The access method is the same (CSMA/CD) for the half-duplex approach; for full- duplex Fast Ethernet, there is no need for CSMA/CD. However, the implementations keep CSMA/CD for backward compatibility with Standard Ethernet.

GIGABIT ETHERNET

The need for an even higher data rate resulted in the design of the Gigabit Ethernet protocol (1000 Mbps). The IEEE committee calls the Standard 802.3z. The goals of the Gigabit Ethernet design can be summarized as follows:

1. Upgrade the data rate to 1Gbps.
2. Make it compatible with Standard or Fast Ethernet.
3. Use the same 48-bitaddress.
4. Use the same frame format.
5. Keep the same minimum and maximum frame lengths.
6. To support auto negotiation as defined in Fast Ethernet.

Ten-Gigabit Ethernet

The IEEE committee created Ten-Gigabit Ethernet and called it Standard 802.3ae.

The goals of the Ten-Gigabit Ethernet design can be summarized as follows:

1. Upgrade the data rate to 10Gbps.
2. Make it compatible with Standard, Fast, and Gigabit Ethernet.
3. Use the same 48-bitaddress.
4. Use the same frame format.
5. Keep the same minimum and maximum frame lengths.
6. Allow the interconnection of existing LANs into a metropolitan area network (MAN) or a wide area network(WAN).

7. Make Ethernet compatible with technologies such as Frame Relay and ATM.

MAC Sublayer

Ten-Gigabit Ethernet operates only in full duplex mode which means there is no need for contention; CSMA/CD is not used in Ten-Gigabit Ethernet.

Physical Layer

The physical layer in Ten-Gigabit Ethernet is designed for using fiber-optic cable over long distances. Three implementations are the most common: 10GBase-S, 10GBase-L, and 10GBase- E.

6. Token Ring (IEEE 802.5)

Token Ring: A Brief History

Originally, IBM developed Token Ring network in the 1970s. It is still IBM's primary local-area network (LAN) technology. The related IEEE 802.5 specification is almost identical to and completely compatible with IBM's Token Ring network. In fact, the IEEE 802.5 specification was modeled after IBM Token Ring, and on the same lines. The term *Token Ring* is generally used to refer to both IBM's Token Ring network andIEEE802.5 networks.

Before going into the details of the Token Ring protocol, let’s first discuss the motivation behind it. As already discussed, the medium access mechanism used by Ethernet (CSMA/CD) may results in collision. Nodes attempt to a number of times before they can actually transmit, and even when they start transmitting there are chances to encounter collisions and entire transmission need to be repeated. And all this become worse one the traffic is heavy i.e. all nodes have some data to transmit. Apart from this there is no way to predict either the occurrence of collision or delays produced by multiple stations attempting to capture the link at the same time. So all these problems with the Ethernet gives way to an alternate LAN technology, Token Ring.

Token Ring and IEEE802.5 are based on token passing MAC protocol with ring topology. They resolve the uncertainty by giving each station a turn on by one. Each node takes turns sending the data; each station may transmit data during its turn. The technique that coordinates this turn mechanism is called Token passing; as a Token is passed in the network and the station that gets the token can only transmit. As one node transmits at a time, there is no chance of collision. We shall discuss the detailed operation in next section.

Stations are connected by point-to-point links using repeaters. Mainly these links are of shielded twisted-pair cables. The repeaters function in two basic modes: Listen mode, Transmit mode. A disadvantage of this topology is that it is vulnerable to link or station failure. But a few measures can be taken to take care of it.

Differences between Token Ring and IEEE 802.5

Both of these networks are basically compatible, although the specifications differin someways. IEEE 802.5 does not specify a topology, although virtually all IEEE802.5 implementations are based on the star topology. While IBM's Token Ring network explicitly specifies a star, with all end stations attached to a device called a Multi- Station Access Unit (MSAU).IEEE 802.5 does not specify a media type, although IBM Token Ring network suse twisted-pair wire. The most common local area network alternative to Ethernet is a network technology developed by IBM, called tokenring. Where Ethernet relies on the random gaps between transmissions to regulate access to the medium, token ring implements a strict, orderly access method.

A token-ring network arranges nodes in a logical ring, as shown below. The nodes forward frames in one direction around the ring,removing a frame when it has circled the ring once. The ring initializes by creating a **token**, which is a special type of frame that gives a station permission to transmit. The token circles the ring like any frame until it encounters a station that wishes to transmit data. This station then "captures" the token by replacing the token frame with a data- carrying frame, which encircles the network. Once that data frame returns to the transmitting station, that station removes the data frame, creates a new token and forwards that token on to the next node in the ring.
Token-ring nodes do not look for a carrier signal or listen for collisions; the presence of the token frame provides assurance that the station can transmit a data frame without fear of another station interrupting. Because a station transmits only a single data frame before passing the token along, each station on the ring will get a turn to communicate in a deterministic and fair manner. Token- ring networks typically transmit data at either 4 or 16Mbps.There are few differences in routing information field size of the two.

Token Ring Operation

Token-passing networks move a small frame, called a *token*, around the network. Possession of the token grants the right to transmit. If a node receiving the token has no information to send, it passes the token to the next end station. Each station can hold the token for a maximum period of time.If a station possessing the token does have information to transmit, it seizes the token, alters 1 bit of the token (which turns the token into a start-of-frame sequence), appends the information that it wants to transmit, and sends this information to the next station on the ring. While the information frame is circling the ring, no token is on the network (unless the ring supports early token release), which means that other stations wanting to transmit must wait. Therefore, *collisions cannot occur in Token Ring networks*. If *early token release* is supported, a new token can be released immediately after a frame transmission iscomplete.

The information frame circulates around the ring until it reaches the intended destination station, which copies the information for further processing. The information frame makes a round trip and is finally removed when it reaches the sending station. The sending station can check the returning frame to see whether the frame was seen and subsequently copied by the destination station in error-free form. Then the sending station inserts a new free token on the ring, if it has finished transmission of itspackets.

Unlike CSMA/CD networks (such as Ethernet), token-passing networks are *deterministic*, which means that it is possible to calculate the maximum time that will pass before any end station will be capable of transmitting. Token Ring networks are ideal for applications in which delay must be predictable and robust network operation is important.

Priority System

Token Ring networks use a sophisticated priority system that permits certain user- designated, high-priority stations to use the network more frequently. Token Ring frames have two fields that control priority: *the priority field* and the *reservation field.*Only stations with a priority equal to or higher than the priority value contained in a token can seize that token. After the token is seized and changed to an information frame, only stations with a priority value higher than that of the transmitting station can reserve the token for the next pass around the network. When the next token is generated, it includes the higher priority of the reserving station. Stations that raise a token's priority level must reinstate the previous priority after their transmission is complete.

Ring Maintenance

There are two error conditions that could cause the token ring to break down. One is the *lost token* in which case there is no token the ring, the other is the *busy token* that circulates endlessly. To overcome these problems, the IEEE 802 standard specifies that one of the

stations be designated as 'active monitor'. The monitor detects the lost condition using a timer by *time-out* mechanism and recovers by using a new free token. To detect a circulating busy token, the monitor sets a 'monitor bit' to one on any passing busy token. If it detects a busy token with the monitor bit already set, it implies that the sending station has failed to remove its packet and recovers by changing the busy token toafreetoken.Otherstationsontheringhavetheroleofpassivemonitor.Theprimaryjob of these stations is to detect failure of the active monitor and assume the role of active monitor. A contention-resolution is used to determine which station to take over.

Physical Layer

The Token Ring uses shielded twisted pair of wire to establish point-point links between the adjacent stations. The baseband signaling uses differential Manchester encoding. To overcome the problem of cable break or network failure, which brings the entire network down, one suggested technique, is to use *wiring concentrator* as shown in Fig. 26.

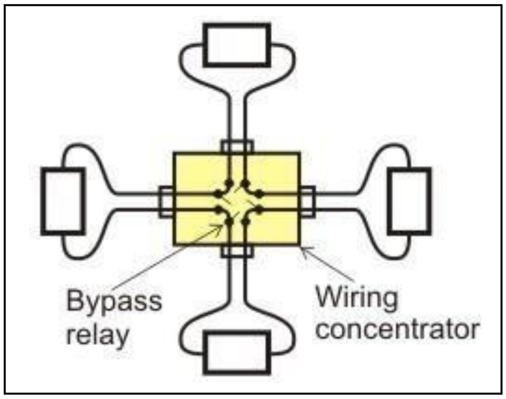


Fig 26 Star Connected Ring topology

It imposes the reliability in an elegant manner. Although logically the network remains as a ring, physically each station is connected to the *wire center* with two twisted pairs for
2- way communication. Inside the wire center, *bypass relays* are used to isolate a broken wire or a faulty station. This Topology is known as Star-Connected Ring**.**

Frame Format

Token Ring and IEEE 802.5 support two basic frame types: tokens and data/command frames. Tokens are 3 bytes in length and consist of a start delimiter, an access control byte, and an end delimiter. Data/command frames vary in size, depending on the size of the Information field. Data frames carry information for upper-layer protocols, while command frames contain control information and have no data for upper-layer protocols.

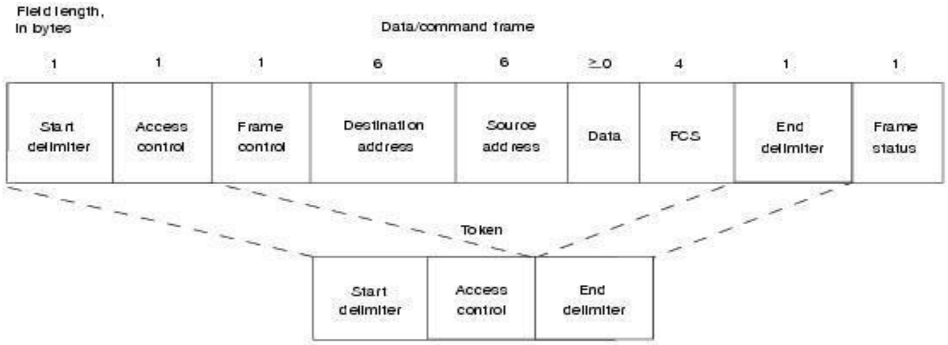


Fig 27 Frame format

Token Ring and IEEE support two basic frame types:

- Tokens
- data/command frames

Tokens are 3 bytes in length and consist of a start delimiter, an access control byte, and an end delimiter. Data/command frames vary in size, depending on the size of the Information field. Data frames carry information for upper-layer protocols, while command frames contain control information and have no data for upper-layer protocols. IEEE 802.5 and Token Ring Specify Tokens and Data/Command Frames

Token Frame Fields

Start	**Access**	**Ending**

Token Frame contains three fields, each of which is 1 byte in length:

- **Start delimiter (1 byte)**: Alerts each station of the arrival of a token (or data/command frame). This field includes signals that distinguish the byte from the rest of the frame by violating the encoding scheme used elsewhere in the frame.
- **Access-control (1 byte)**: Contains the Priority field (the most significant 3 bits) and the Reservation field (the least significant 3 bits), as well as a token bit (used to differentiate a token from a data/command frame) and a monitor bit (used by the active monitor to determine whether a frame is circling the ring endlessly).
- **End delimiter (1 byte)**: Signals the end of the token or data/command frame. This field also contains bits to indicate a damaged frame and identify the frame that is the last in a logica lsequence.

Data/Command Frame Fields

Start Delimiter	**Access Contr**	**Frame Contr**	**Destination address**	**Source addre**	**Data**	**Frame check sequence**	**End Delimiter**	**Frame Stat**

Data/command frames have the same three fields as Token Frames, plus several others. The Data/command frame fields are described below:

- **Frame-control byte (1 byte)**—Indicates whether the frame contains data or control information. In control frames, this byte specifies the type of control information.
- **Destination and source addresses (2-6 bytes)**—Consists oftwo6-bytaddress fields that identify the destination and source station addresses.
- **Data (up to 4500 bytes)**—Indicates that the length of field is limited by the ring token holding time, which defines the maximum time a station can hold thetoken.
- **Frame-check sequence (FCS- 4 byte)**—Is filed by the source station with a calculated value dependent on the frame contents. The destination station recalculates the value to determine whether the frame was damaged in transit. If so, the frame is discarded.
- **Frame Status (1 byte)**—This is the terminating field of a command/data frame. The Frame Status field includes the address-recognized indicator and frame-copied indicator.

Token Frame Fields

The three token frame fields descriptions that follow:

- **Start delimiter** - Alerts each station of the arrival of a token (or data/command frame). This field includes signals that distinguish the byte from the rest of the frame by violating the encoding scheme used elsewhere in the frame.
- **Access-control byte** - Contains the Priority field (the most significant 3 bits) and the Reservation field (the least significant 3 bits), as well as a token bit (used to differentiate a token from a data/command frame) and a monitor bit (used by the active monitor to determine whether a frame is circling the ring endlessly).

- **End delimiter** - Signals the end of the token or data/command frame. This field also contains bits to indicate a damaged frame and identify the frame that is the last in a logical sequence.

Data/Command Frame Fields

Data/command frames have the same three fields as Token Frames, plus several others. The Data/command frame fields are described in the following summaries:

- **Start delimiter** - Alerts each station of the arrival of a token (or data/command frame). This field includes signals that distinguish the byte from the rest of the frame by violating the encoding scheme used elsewhere in the frame.
- **Access-control byte** - Contains the Priority field (the most significant 3 bits) and the Reservation field (the least significant 3 bits), as well as a token bit (used to differentiate a tokenfromadata/commandframe)andamonitorbit(usedbytheactivemonitortodetermine whether a frame is circling the ring endlessly).

- **Frame-control bytes** - Indicates whether the frame contains data or control information. In control frames, this byte specifies the type of control information.
- **Destination and source addresses** - Consists of two 6-byte address fields that identify the destination and source station addresses.
- **Data** - Indicates that the length of field is limited by the ring token holding time, which defines the maximum time a station can hold the token.
- **Frame-check sequence (FCS)** - Is filed by the source station with a calculated value dependent on the frame contents. The destination station recalculates the value to determine whether the frame was damaged in transit. If so, the frame is discarded.
- **End Delimiter** - Signals the end of the token or data/command frame. The end delimiter also contains bits to indicate a damaged frame and identify the frame that is the last in a logical sequence.
- **Frame Status** - Is a 1-byte field terminating a command/data frame. The Frame Status field

includes the address-recognized indicator and frame-copied indicator.

7. Token Bus (IEEE 802.4)

Token BUS: A Brief History

Although Ethernet was widely used in the offices, but people interested in factory automation did not like it because of the probabilistic MAC layer protocol. They wanted a protocol which can support priorities and has predictable delay. These people liked the conceptual idea of Token Ring network but did not like its physical implementation as a break in the ring cable could bring the whole network down and ring is a poor fit to their linear assembly lines. Thus a new standard, known as Token bus, was developed, having therobustnessoftheBustopology,buttheknownworst-casebehaviorofaring.Here stations are logically connected as a ring but physically on a Bus and follows the collision-free token passing medium access control protocol. So the motivation behind token bus protocol can be summarized as:

- The probabilistic nature of CSMA/ CD leads to uncertainty about the delivery time; which created the need for a different protocol
- The token ring, on the hand, is very vulnerable to failure.
- Token bus provides deterministic delivery time, which is necessary for real time traffic.
- Token bus is also less vulnerable compared to token ring.

Functions of a Token Bus

It is the technique in which the station on bus or tree forms a logical ring, that is the stations are assigned positions in an ordered sequence, with the last number of the sequence followed by the first one as shown in Figure. Each station knows the identity of the station following it and preceding it.

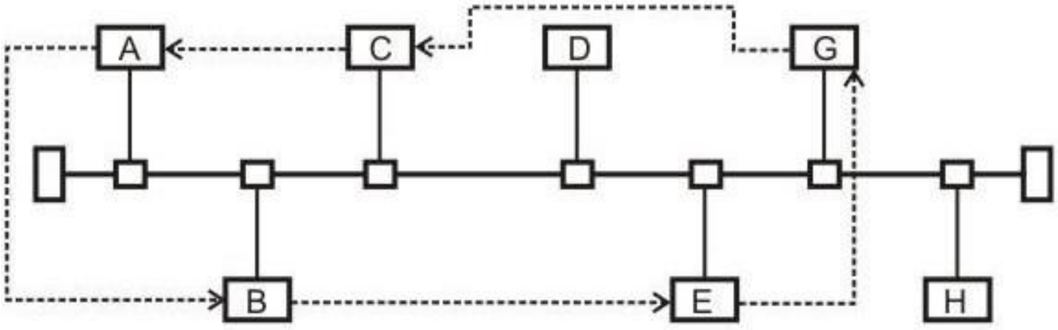


Fig 28 Token Bus topology

A control packet known as a *Token* regulates the right to access. When a station receives the token, it is granted control to the media for a specified time, during which it may transmit one or more packets and may poll stations and receive responses when the station is done, or if its time has expired then it passes token to next station in logical sequence. Hence, steady phase consists of alternate phases of token passing and data transfer.

The MAC sublayer consists of four major functions: the interface machine (IFM), the access control machine (ACM), the receiver machine (RxM) and the transmit machine (TxM).

IFM interfaces with the LLC sublayer. The LLC sublayer frames are passed on to the ACM by the IFM and if the received frame is also an LLC type, it is passed from RxM component to the LLC sublayer. IFM also provides quality of service.

The **ACM** is the heart of the system. It determines when to place a frame on the bus, and responsible for the maintenance of the logical ring including the error detection and fault recovery. It also cooperates with other stations ACM’s to control the access to the shared bus, controls the admission of new stations and attempts recovery from faults and failures.

The responsibility of a **TxM** is to transmit frame to physical layer. It accepts the frame from the ACM and builds a MAC protocol data unit (PDU) as per the format.

The **RxM** accepts data from the physical layer and identifies a full frame by detecting the SD and ED (start and end delimiter). It also checks the FCS field to validate an error- free transmission.

Frame Form

The frame format of the Token Bus is shown in Figure. Most of the fields are sameas Token Ring.

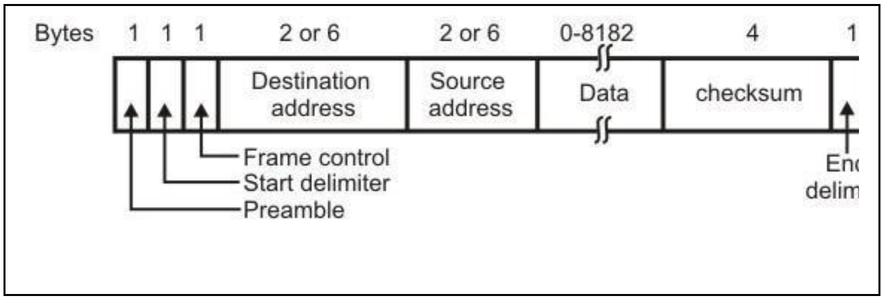


Fig 29 Token Bus frame format

Logical ring maintenance

The MAC performs the following functions as part of its maintenance role of the ring.

Addition to the Ring: Non-participating stations must periodically be granted the opportunity to insert themselves into the ring. Each node in the ring periodically grants an opportunity for new nodes to enter the ring while holding the token. The node issues a solicit–successor–1 packet, inviting nodes with an address between itself and the nextnode in logical sequence to request entrance. The transmitting node then waits for a period of time equal to one response window or slot time (twice the end-to-end propagation delay of the medium). If there is no request, the token holder sets its successor node to be the requesting node and transmits the token to it; the requester sets the linkages accordingly and proceeds.

If more than one node requests, to enter the ring, the token holder will detect a garbled transmission. The conflict is resolved by *addressed based contention scheme;* the token holder transmits a resolved contention packet and waits for four response windows. Each requester can transmit in one of these windows, based on the first two bits of its address. If requester hears anything before its windows comes up, it refrains from requesting entrance. If a token holder receives a valid response, then it can proceed, otherwise it tries again and only those nodes that request the first time are allowed to request this time, based on the second pair of bits in their address. This process continues until a valid request is received or no request is received, or a maximum retry count is reached. In latter cases, the token holder passes the token to logical successor in the ring.

Deletion from Ring: A station can voluntarily remove itself from the ring by splicing together its predecessor and successor. The node which wants to be deleted from the ring waits until token comes to it, then it sends a set successor packet to its predecessor, instructing it to splice to its successor.

Fault Management: Errors like duplicate address or broken ring can occur. A suitable management scheme should be implemented for smooth functioning. It is done by the token-holder first, while holding the token, node may hear a packet, indicating that another node has the token. In this case, it immediately drops the token by reverting to listener mode, and the number of token holders drops immediately from one to zero. Upon completion of its turn, it immediately issues a data or token packet. The sequence of steps are as follows:

i. After sending the token, the token issuer will listen for one slot time to make sure that its predecessor is active.
ii. If the issuer does not hear a valid packet, it reissues the token to the same successor one more time.
iii. After two failures, the issuer assumes that its successor has failed and issues a "who-follows" packet, asking for the identity of the node that follows the failed node. The issuer should get back a set successor packet from the second node down the time. If so, the issuer adjusts its linkage and issues a token .
iv. If the issuing node gets a response to its "who-follows" packet, it tries again.
v. If the "who-follows" tactic fails, the node issues a solicit-successor-2 packet with full address range (i.e. every node is invited to respond). If this packet works then the ring is established and procedure continues.
vi. If two attempts in step (v) fail, it assumes that a catastrophe has happened; perhaps the node receiver has failed. In any case, the node ceases the activity and listen the bus.

Ring Initialization: Ring is to be initialized by starting the token passing. This is necessary when the network is being setup or when ring is broken down. Some decentralized algorithms should take care of, who starts first, who starts second, etc. it occurs when one or more stations detects a lack of bus activity lasting longer than a specific time. The token may get lost. This can occur on a number of occasions. For example, when network has been just powered up, or a token holding station fails. Once its time out expires, a node will issue a claim token packet. Contending clients are removed in a similar fashion to the response window process.

Relative comparison of the three standards

A comparison of the three standards for different functions is shown in Table and results of the analysis of the performance of the three standards are summarized below:

The CSMA/CD protocol shows strong dependence on the parameter 'a', which is the ratio of the propagation time to the transmission time. It offers shortest delay under light load and it is most sensitive under heavy load conditions.

Token ring is least sensitive to different load conditions and different packet sizes.

Token bus is highly efficient under light load conditions

8. SMDS

Switched Multimegabit Data Service (SMDS) is a packet-switched datagram service designed for very high-speed wide-area data communications. SMDS offers data throughputs that will initially be in the 1- to 34-Mbps range.

Ethernet

SMDS data units are capable of containing up to 9,188 octets (bytes) of user information. SMDS is therefore capable of encapsulating entire IEEE 802.3, IEEE 802.4, IEEE 802.5, and FDDI frames. The large packet size is consistent with the high-performance objectives of the service.

Addressing

Like other datagram protocols, SMDS data units carry both a source and a destination address. The recipient of a data unit can use the source address to return data to the sender and for functions such as address resolution (discovering the mapping between higher-layer addresses and SMDS addresses). SMDS addresses are 10-digit addresses that resemble conventional telephone numbers. In addition, SMDS supports group addresses that allow a single data unit to be sent and then delivered by the network to multiple recipients. Group addressing is analogous to multicasting on local-area networks (LANs) and is a valuable feature in internetworking applications where it is widely used for routing, address resolution, and dynamic discovery of network resources.

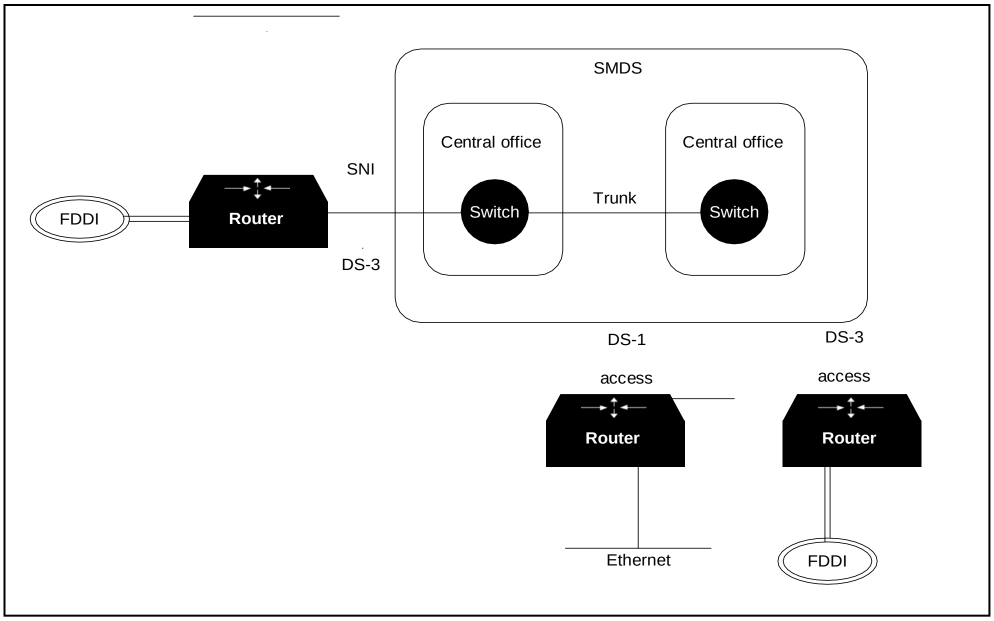


Fig 30 SMDS Operation

SMDS offers several other addressing features. Source addresses are validated by the network to ensure that the address in question is legitimately assigned to the SNI from which it originated. Thus, users are protected against address spoofing—that is, a sender pretending to be another user. Source and destination address screening is also possible. Source address screening acts on addresses as data units are leaving the network, while destination address screening acts on addresses as data units are entering the network. If the address is disallowed, the data unit is not delivered. With address screening, a subscriber can establish a private virtual network that excludes unwanted traffic.

SMDS data units are capable of containing up to 9,188 octets (bytes) of user information. SMDS is therefore capable of encapsulating entire IEEE 802.3, IEEE 802.4, IEEE 802.5, and FDDI frames. The large packet size is consistent with the high-performance objectives of the service.

Access Classes

To accommodate a range of traffic requirements and equipment capabilities, SMDS supports a variety of access classes. Different access classes determine the various maximum sustained information transfer rates as well as the degree of burstiness allowed when sending packets into the SMDS network.

On DS-3-rate interfaces, access classes are implemented through credit management algorithms, which track credit balances for each customer interface. Credit is allocated on a periodic basis, up to some maximum. Then, the credit balance is decremented as packets are sent to the network.

The operation of the credit management scheme essentially constrains the customer's equipment to some sustained or average rate of data transfer. This average rate of transfer is less than the full information carrying bandwidth of the DS-3 access facility. Five access classes, corresponding to sustained information rates of 4, 10, 16, 25, and 34 Mbps, are supported for DS-3 access interface. The credit management scheme is not applied to DS-1-rate access interfaces.

SMDS Interface Protocol (SIP)

Access to the SMDS network is accomplished via SIP. The SIP is based on the DQDB protocol specified by the IEEE 802.6 MAN standard. The DQDB protocol defines a Media Access Control (MAC) protocol that allows many systems to interconnect via two unidirectional logical buses.

As designed by IEEE 802.6, the DQDB standard can be used to construct private, fiber-based MANs supporting a variety of applications including data, voice, and video. This protocol was chosen as the basis for SIP because it was an open standard, could support all the SMDS service features, was designed for compatibility with carrier transmission standards, and is aligned with emerging standards for Broadband ISDN (BISDN). As BISDN technology matures and is deployed, the carriers intend to support not only SMDS but broadband video and voice services as well.

To interface to SMDS networks, only the connectionless data portion of the IEEE 802.6 protocol is needed. Therefore, SIP does not define voice or video application support.

When used to gain access to an SMDS network, operation of the DQDB protocol across the SNI results in an access DQDB. The term access DQDB distinguishes operation of DQDB across the SNI from operation of DQDB in any other environment (such as inside the SMDS network). A switch in the SMDS network operates as one station on an access DQDB, while customer equipment operates as one or more stations on the access DQDB.

Because the DQDB protocol was designed to support a variety of data and nondata applications and because it is a shared medium access control protocol, it is relatively complex. It has two parts:

- The protocol syntax
- The distributed queuing algorithm that constitutes the shared medium access control

9. Fiber-Distributed Data Interface (FDDI)

Introduction

The IEEE 802.3 and 802.5 LANs, discussed in the previous sections, having data transfer rate in the range of 10 Mb/s to 16 Mb/s have served the purpose very well for many years. But with the availability of powerful computers at a low cost and emergence of new applications, particularly based on multimedia, there is a growing demand for higher network bandwidth. The combined effect of the growth in the number of users and increasing bandwidth requirement per user has led to the development of High Speed. LANs with data transfer rate of 100 Mb/s or more.

The high speed LANs that have emerged can be broadly categorized into three types *based on token passing*, *successors of Ethernet* and *based on switching technology*. In the first category we have *FDDI* and its variations, and high-speed token ring. In the second category we have the *fast Ethernet* and *Gigabit Ethernet*. In the third category we have *ATM*, *fiber channel* and the *Ether switches*. In this lesson we shall discuss details of FDDI – the token ring based high speed LAN.

FDDI

Fiber Distributed Data Interface (FDDI), developed by American National Standards Institute (ANSI) is a token passing ring network that operates at 100 Mb/s on optical fiber-medium. Its medium access control approach has close similarity with the IEEE
802.5 standard, but certain features have been added to it for higher reliability and better performance. Key features of FDDI are outlined in this section.

The FDDI standard divides transmission functions into 4 protocols: physical medium dependent (PMD), Physical (PHY), media access control(MAC) and Logical link control(LLC) as shown in Fig. These protocols correspond to the physical and data link layer of OSI reference model. Apart from these four protocols, one more protocol which span across both data link and physical layer (if considered of OSI), used for the station management.

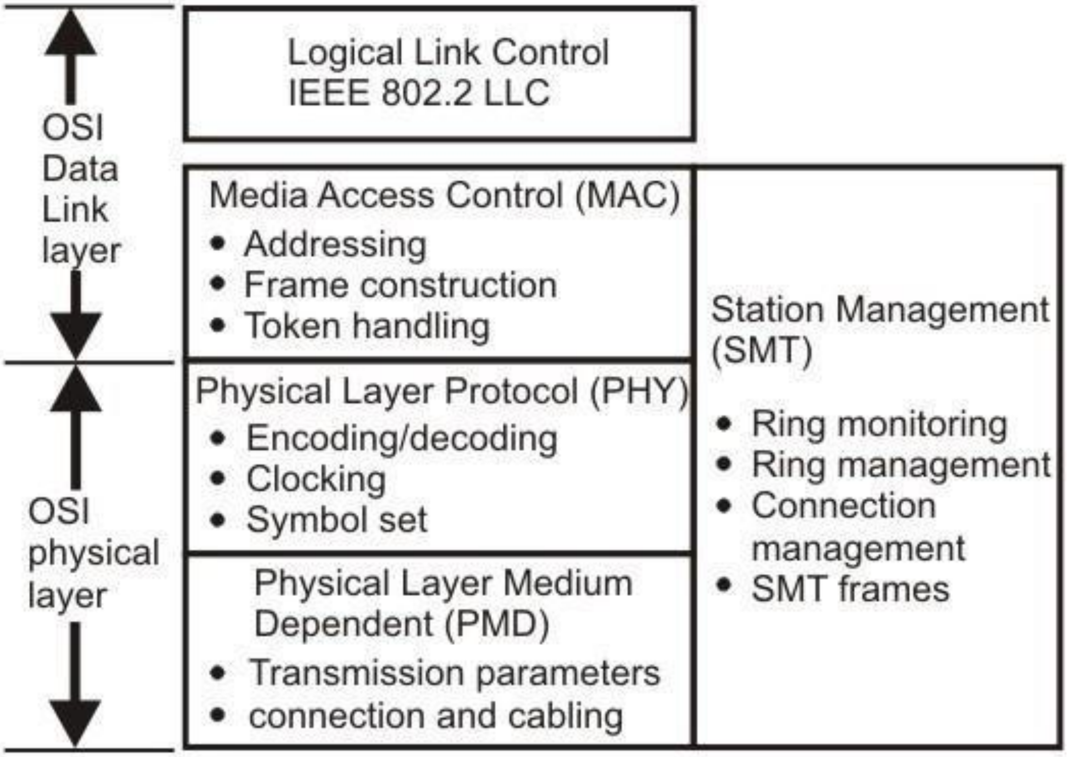


Fig 31 FDDI protocols

FDDI networks offered transmission speeds of 100 Mbps, which initially made them quite popular for high-speed networking. With the advent of 100-Mbps Ethernet, which is
cheaper and easier to administer, FDDI has waned in popularity.

FDDI (Fiber-Distributed Data Interface) is a standard for data transmission on fiber optic lines in that can extend in range up to 200 km (124 miles). The FDDI protocol is based on the token ring protocol. In addition to being large geographically, an FDDI local area network can support thousands of users.

An FDDI network contains two token rings, one for possible backup in case the primary ring fails. The primary ring offers up to 100 Mbps capacity. If the secondary ring is not needed for backup, it can also carry data, extending capacity to 200 Mbps. The single ring can extend the maximum distance; a dual ring can extend 100 km (62miles).

FDDI is a product of American National Standards Committee X3-T9 and conforms to the open system interconnect (OSI) model of functional layering. It can be used to interconnect LANs using other protocols.

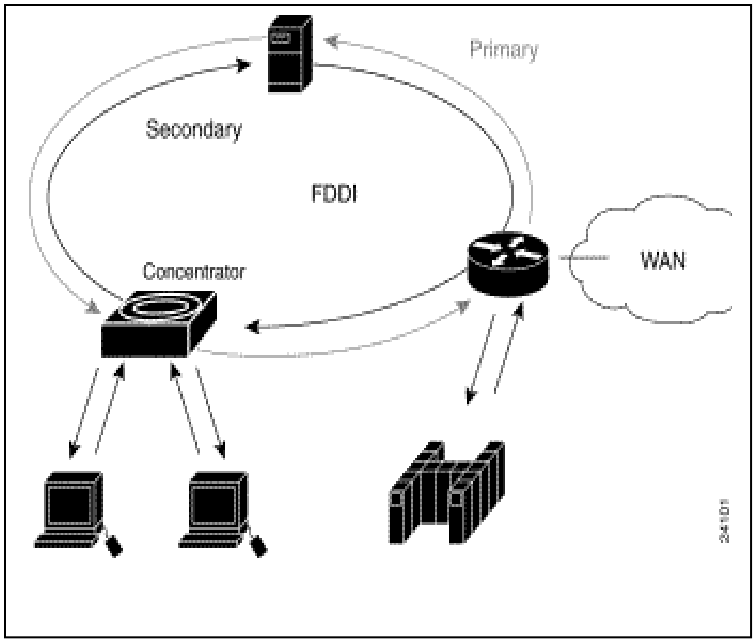


Fig 31 FDDI Operation

Function of FDDI

- The Fiber Distributed Data Interface (FDDI) specifies a 100-Mbps token-passing, dual-ring LAN using fiber-optic cable. FDDI is frequently used as high-speed backbone technology because of its support for high bandwidth and greater distances than copper.
- FDDI uses a dual-ring architecture with traffic on each ring flowing in opposite directions (called counter- rotating).
- The dual-rings consist of a primary and a secondary ring.
- During normal operation, the primary ring is used for data transmission, and the secondary

ring remains idle.

- The primary purpose of the dual rings, as will be discussed in detail later in this chapter, is to provide superior reliability and robustness. Figure 1 shows the counter-rotating primary and secondary FDDI rings.

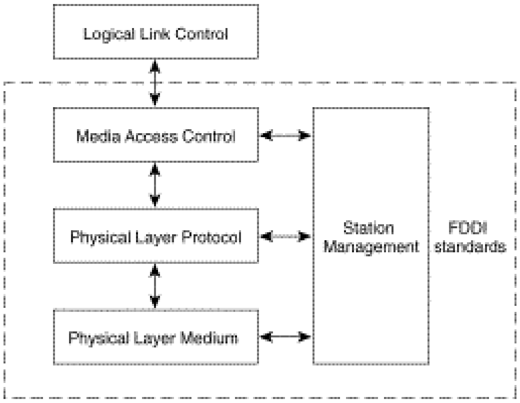


Fig 32 Layers of FDDI

FDDI Station-Attachment Types

One of the unique characteristics of FDDI is that multiple ways actually exist by which to connect FDDI devices. FDDI defines three types of devices: single-attachment station (SAS), dual-attachment station (DAS), and a concentrator.

An SAS attaches to only one ring (the primary) through a concentrator. One of the primary advantages of connecting devices with SAS attachments is that the devices will not have any effect on the FDDI ring if they are disconnected or powered off. Concentrators will be discussed in more detail in the following discussion. Each FDDI DAS has two ports, designated A and B. These ports connect the DAS to the dual FDDI ring. Therefore, each port provides a connection for both the primary and the secondary ring. As you will see in the next section, devices using DAS connections will affect the ring if they are disconnected or powered off. Figure 3 shows FDDI DAS A and B ports with attachments to the primary and secondary rings. An FDDI concentrator (also called a dual-attachment concentrator [DAC]) is the building block of an FDDI network. It attaches directly to both the primary and secondary rings and ensures that the failure or power-down of any SAS does not bring down the ring.

FDDI Physical layer specification

FDDI uses 4B/5B code for block coding. The 5-bit code is selected such that it has no more than one leading zero and no more than two trailing zeros and more than three consecutive 0's do not occur. Table 5.5.2 shows the encoded sequence for all the 4-bit data sequences. The This is normally line coded with NRZ-I.

Topology

The basic topology for FDDI is *dual counter rotating rings:* one transmitting clockwise and the other transmitting counter clockwise as illustrated in the Fig. One is known as *primary ring* and the other *secondary ring*. Although theoretically both the rings can be used to achieve a data transfer rate of 200 Mb/s, the standard recommends the use of the primary ring for data transmission and secondary ring as a backup.

In case of failure of a node or a fiber link, the ring is restored by wrapping the primary ring to the secondary ring. The redundancy in the ring design provides a degree of fault tolerance, not found in other network standards. Further improvement in reliability and availability can be achieved by using *dual ring* of trees and *dual homing* mechanism.

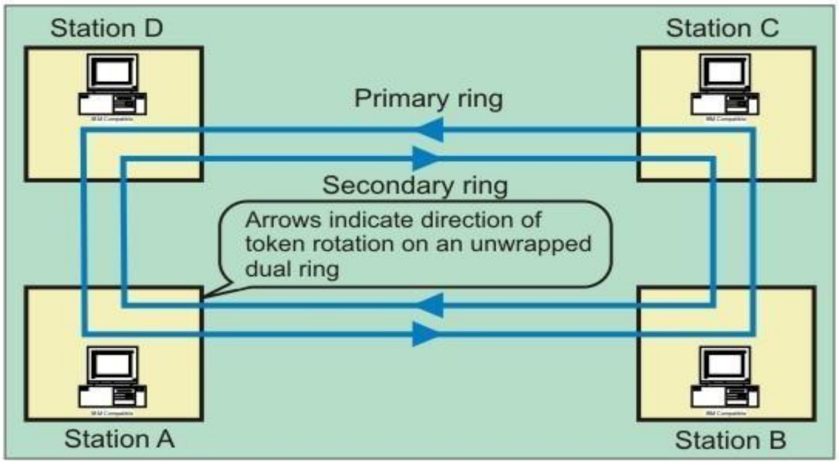

Station D
Station C
Primary ring
Secondary ring
Arrows indicate direction of token rotation on an unwrapped dual ring
Station A
Station B

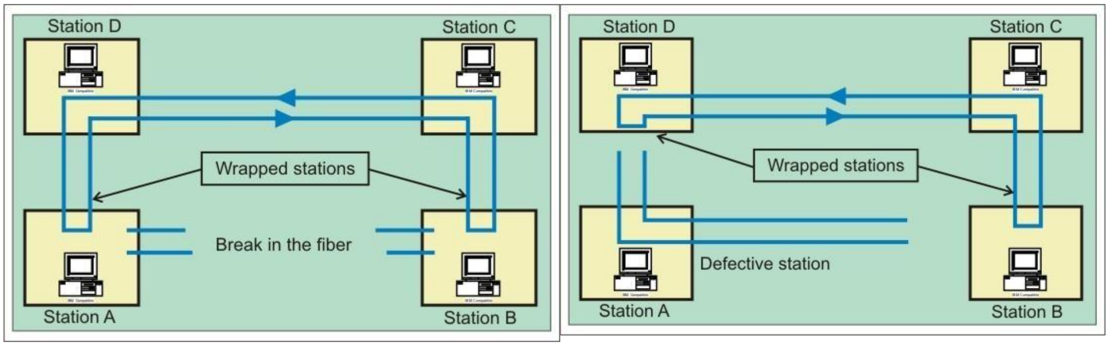
Fig 33 FDDI dual counter-rotating ring topology

Fault Tolerance

FDDI provides a number of fault-tolerant features. In particular, FDDI's dual-ring environment, the implementation of the optical bypass switch, and dual-homing support make FDDI a resilient media technology.

Dual Ring

FDDI's primary fault-tolerant feature is the *dual ring*. If a station on the dual ring fails or is powered down, or if the cable is damaged, the dual ring is automatically wrapped (doubled back onto itself) into a single ring. When the ring is wrapped, the dual-ring topology becomes a single-ring topology. Data continues to be transmitted on the FDDI ring without performance impact during the wrap condition. Figure (a) and Figure (b) illustrate the effect of a ring wrapping in FDDI.



(b)

Fig 34 FDDI ring with a (a) broken link, (b) defective station

When a cable failure occurs, devices on either side of the cable fault wrap. Network operation continues for all stations. When a single station fails ,devices on either side of the failed (or powered-down) station wrap, forming a single ring. Network operation continues for the remaining stations on the ring. It should be noted that FDDI truly provides fault tolerance against a single failure only. When two or more failures occur, the FDDI ring segments into two or more independent rings that are incapable of communicating with eachother.

Optical Bypass Switch

An optical bypass switch provides continuous dual-ring operation if a device on the dual ring fails. This is used both to prevent ring segmentation and to eliminate failed stations from the ring. The optical bypass switch performs this function using optical mirrors that pass light from the ring directly to the DAS (dual-attachment station) device during normal operation. If a failure of the DAS device occurs, such as a power-off, the optical bypass switch will pass the light through itself by using internal mirrors and thereby will maintain the ring's integrity.

Failed Station

The benefit of this capability is that the ring will not enter a wrapped condition incase of a device failure. A somewhat similar technique has been discussed in Token ring section (Star Connected Ring- where relays are used to bypass the faulty node). Figure shows the functionality of an optical bypass switch in an FDDI network. When using the OB, you will notice a tremendous digression of your network as the packets are sent through the OB unit.

Dual Homing: Critical devices, such as routers or mainframe hosts, can use a fault- tolerant technique called *dual homing* to provide additional redundancy and to help guarantee operation. In dual-homing situations, the critical device is attached to two concentrators.

Frame Format

Each Frame is preceded by a preamble (16 idle symbols-1111), for a total of 64 bits, to initialize clock synchronization with the receiver.

PA:	Preamble
SD:	Starting Delimiter
FC:	Frame Control
DA :	Destination Address
SA:	Source Address
FCS:	Frame Check Sequence
ED:	Ending Delimiter
FS:	Frame Status

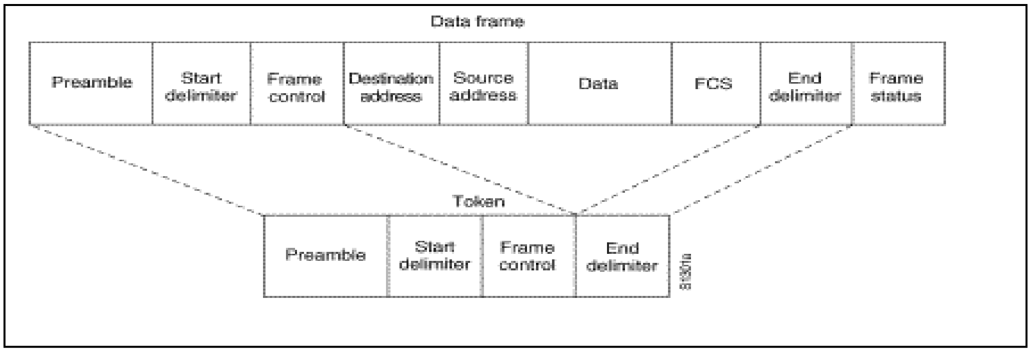


Fig 35 Frame format for the FDDI

Let us have a look at the various fields:
SD: The first byte, after the preamble, of the field is the frame's starting flag. As in Token ring these bits are replaced in physical layer by the control codes.

FC: it identifies the frame type i.e. token or a data frame.
Address: the next 2 fields are destination and source addresses. Each address consists of 2-6 bytes.

Data: Each data frame carries up to 4500 bytes.

FCS: FDDI uses the standard IEEE four-byte cyclic redundancy check.
ED: this field consists of half a byte in data frame or a full byte in token frame. This represents end of the Token.

FS: FDDI FS field is similar to that of Token Ring. It is included only in data/Command frame and consists of one and a half bytes.

Media Access Control

The FDDI media access control protocol is responsible for the following services.

(i) Fair and equal access to the ring by using a *timed token protocol*. To transmit on the ring, a station must first acquire the token. A station holds the token until it has transmitted all of its frames or until the transmission time for the appropriate service is over. Synchronous traffic is given a guaranteed bandwidth by ensuring that token rotation time does not exceed a preset value. FDDI implements these using three timers, *Token holding Timer* (THT), which determines how long a station may continue once it has captured a token. *Token Rotation Timer* (TRT) is reset every time a token is seen. When timer expires, it indicates that the token is lost and recovery is started. The Valid Transmission Timer (VTT) is used to time out and recover from some transmit ring errors.

(ii) Construction of frames and tokens are done as per the format shown in Figure 5.5.5. The frame status (FS) byte is set by the destination and checked by the source station, which removes its frame from the ring and generates another token.

(iii) Transmitting, receiving, repeating and stripping frames and tokens from the ring, unlike IEEE 802.5, is possible for several frames on the ring simultaneously. Thus a station will transmit a token immediately after completion of its frame transmission. A station further

(iv) down the ring is allowed to insert its own frame. This improves the potential throughput of the system. When the frame returns to the sending station, that station removes the frame from the ring by a process called *stripping*.

(v) It also does *ring initialization*, *fault isolation* and error detection as we have discussed for IEEE802.5.

10. DQDB-IEEE 802.6

The IEEE Standard 802.6 *(*Distributed Queue Dual Bus *(DQDB) Sub network of a* Metropolitan Area Network (MAN)) permits sub network reconfiguration, usually without loss of communication ability, whenever there are bus faults. The Configuration Control Protocol (CCP) is the protocol which enables this to occur.

IEEE 802.6 is a standard governed by the ANSI for Metropolitan Area Networks (MAN). It is an improvement of an older standard (also created by ANSI) which used the Fiber distributed data interface (FDDI) network structure.The FDDI-based standard failed due to its expensive implementation and lack of compatibility with current LAN standards. The IEEE 802.6 standard uses the Distributed Queue Dual Bus (DQDB) network form. This form supports 150 Mbit/s transfer rates. It consists of two unconnected unidirectional buses. DQDB is rated for a maximum of 160 km before significant signal degradation over fiber optic cable with an optical wavelength of1310 nm. This standard has also failed, mostly due to the same reasons that the FDDI standard failed. Most MANs now use Synchronous Optical Network (SONET) or Asynchronous Transfer Mode (ATM) network designs, with recent designs using native Ethernet or MPLS.

<u>The DQDB Physical Layer</u>

The Head of Bus (HOB)s act a slot generators so that the bus is never quiet.Nodes are located logically adjacent to the bus and are promiscuous readers. They read all slots that come off the bus but may not necessarily alter any of the data. Nodes may be passive readers or, in an active system, they may act as repeaters so as to forestall attenuation. If Node 2 wishes to send data in the direction of Node n then it will use Bus A. This implies that it must first reserve a slot by placing a request on Bus B.If Node 2 wishes to send data in the direction of Node 1 it must first reserve a slot using Bus A and then send the data on Bus B.

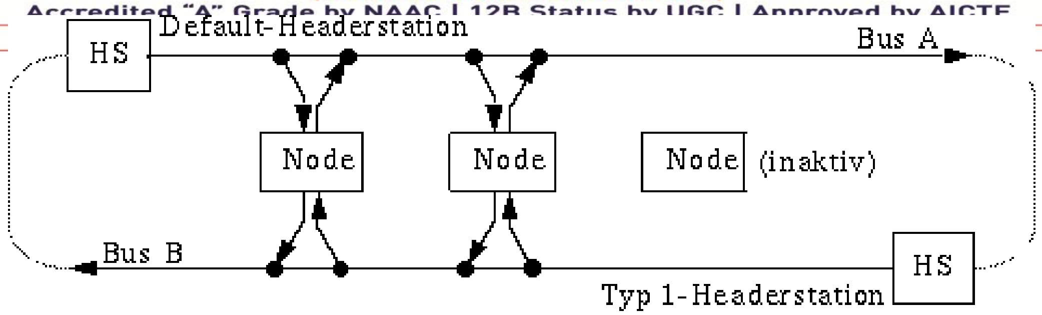


Fig 36 DQDB Operation

DQDB Operation

- The DQDB configuration is independent of the number of nodes and of the distances involved making DQDB ideal for high-speed transmissions
- DQDB uses 53-byte packets (52 data bytes and one access control byte) for transmissions called slots.
  - Slots from different nodes are intermingled in the network traffic.

- The head node (the first node connected to the external fiber) is responsible for creating empty slots and sending these down the line to the other nodes to use.
- The down line nodes indicate how many slots are needed using the secondary bus to the head node which then creates empty slots and sends these down the line.
  - As the slots move down the line, they are taken by the nodes that have requested them.

Switching

A network is a set of connected devices. Whenever we have multiple devices, we have the problem of how to connect them to make one-to-one communication possible. One solution is to make a point-to-point connection between each pair of devices (a mesh topology) or between a central device and every other device (a star topology). These methods, however, are impractical and wasteful when applied to very large networks. The number and length of the links require toomuch infrastructure to be cost-efficient, and the majority of those links would be idle most of the time. Other topologies employing multipoint connections, such as a bus, are ruled out because the distances between devices and the total number of devices increase beyond the capacities of the media and equipment.

A better solution is switching. A switched network consists of a series of interlinked nodes, called switches. Switches are devices capable of creating temporary connections between two or more devices linked to the switch. In a switched network, some of these nodes are connected to the end systems (computers or telephones, for example). Others are used only for routing. Figure shows a switchednetwork.

The end systems (communicating devices) are labeled A, B, C, D, and so on, and the switches are labeled I, II, III, IV, and V. Each switch is connected to multiple links.

Taxonomy of switched networks

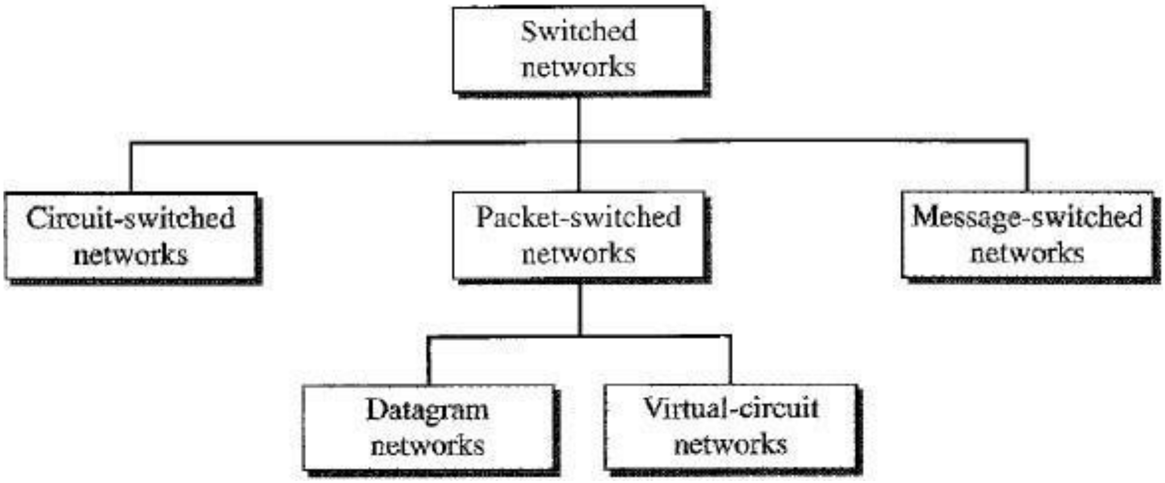


Fig 37 Types of switched Networks

11. CIRCUIT-SWITCHED NETWORKS

A circuit-switched network consists of a set of switches connected by physical links. A connection between two stations is a dedicated path made of one or more links. However, each connection uses only one dedicated channel on each link. Each link is normally divided into *n* channels by using FDM or TDM. Figure shows a trivial circuit-switched network with four switches and four links. Each link is divided into *n* (*n* is 3 in the figure) channels by using

FDM or TDM.

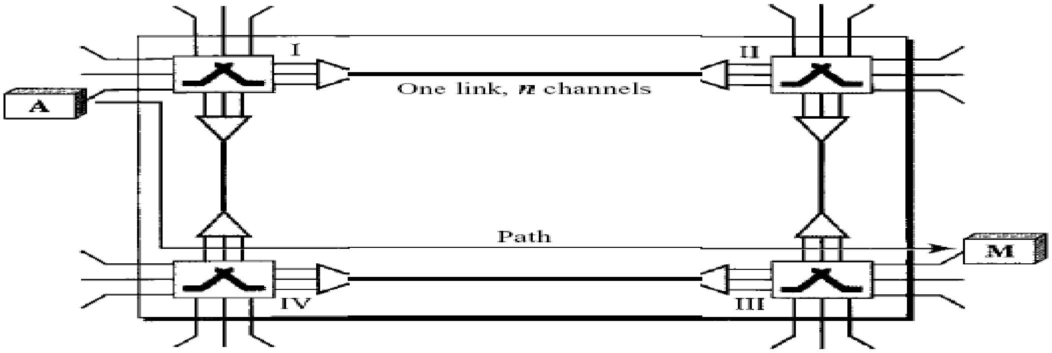


Fig 38 A trivial circuit-switched network

Three Phases

The actual communication in a circuit-switched network requires three phases: connection setup, data transfer, and connection teardown.

Setup Phase*:*

Before the two parties (or multiple parties in a conference call) can communicate, a dedicated circuit (combination of channels in links) needs to be established. The end systems are normally connected through dedicated lines to the switches, so connection setup means creating dedicated channels between the switches. For example, in Figure, when system A needs to connect to system M, it sends a setup request that includes the address of system M, to switch I. Switch I finds a channel between itself and switch IV that can be dedicated for this purpose. Switch I then sends the request to switch IV, which finds a dedicated channel between itself and switch III. Switch III informs system M of system A's intention at this time. In the next step to making a connection, an acknowledgment from system M needs to be sent in the opposite direction to system A. Only after system A receives this acknowledgment is the connection established. Note that end-to-end addressing is required for creating a connection between the two end systems. These can be, for example, the addresses of the computers assigned by the administrator in a TDM network, or telephone numbers in an FDM network.

Data Transfer Phase:

After the establishment of the dedicated circuit (channels), the two parties can

Transfer data.

Teardown Phase:

When one of the parties needs to disconnect, a signal is sent to each switch to release the resources.

Efficiency:

It can be argued that circuit-switched networks are not as efficient as the other two types of networks because resources are allocated during the entire duration of the connection. These resources are unavailable to other connections. In a telephone network, people normally terminate the communication when they have finished their conversation. However, in computer networks, a computer can be connected to another computer even if there is no activity for a long time. In this case, allowing resources to be dedicated means that other connections are deprived.

Delay

Although a circuit-switched network normally has low efficiency, the delay in this type of network is minimal. During data transfer the data are not delayed at each switch; the resources are allocated for the duration of the connection. As Figure shows, there is no waiting time at each switch. The total delay is due to the time needed to create the connection, transfer data, and disconnect the circuit.

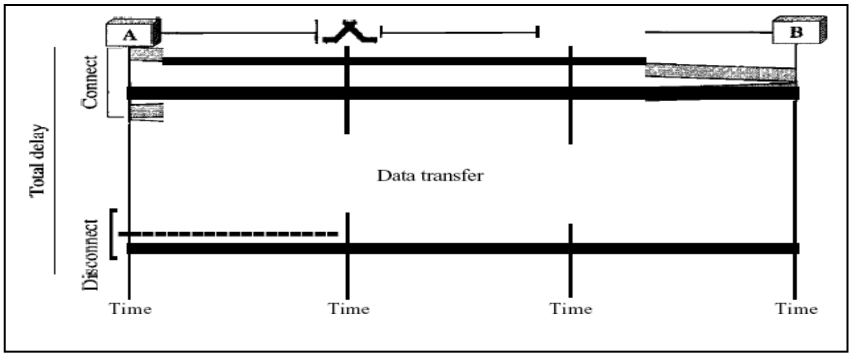


Fig 39 Delay in a circuit-switched network

The delay caused by the setup is the sum of four parts: the propagation time of the source computer request (slope of the first gray box), the request signal transfer time (height of the first gray box), the propagation time of the acknowledgment from the destination computer (slope of the second gray box), and the signal transfer time of the acknowledgment (height of the second gray box). The delay due to data transfer is the sum of two parts: the propagation time (slope of the colored box) and data transfer time (height of the colored box), which can be very long. The third box shows the time needed to tear down the circuit. We have shown the case in which the receiver requests disconnection, which creates the maximum delay.

DATAGRAM NETWORKS

In a datagram network, each packet is treated independently of all others. Even if a packet is part of a multi packet transmission, the network treats it as though it existed alone. Packets in this approach are referred to as datagrams.

Datagram switching is normally done at the network layer. We briefly discuss datagram networks here as a comparison with circuit-switched and virtual-circuit switched networks Figure shows how the datagram approach is used to deliver four packets from station A to station

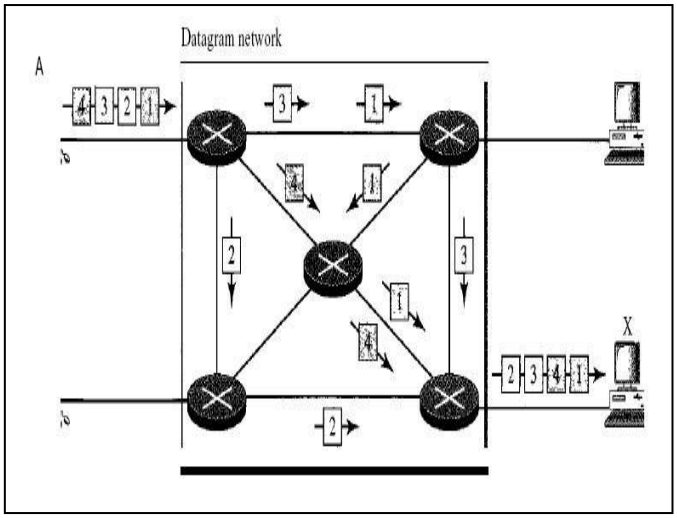


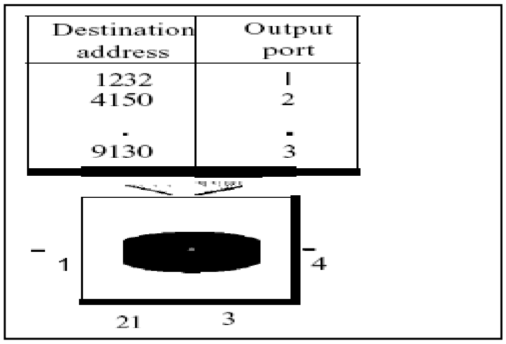
Fig 40 Datagram network with four switches (routers)

The switches in a datagram network are traditionally referred to as routers. That is why we use a different symbol for the switches in the figure. In this example, all four packets (or datagrams) belong to the same message, but may travel different paths to reach their destination. This is so because the links may be involved in carrying packets from other sources and do not have the necessary bandwidth available to carry all the packets from A to X. This approach can cause the datagrams of a transmission to arrive at their destination out of order with different delays between the packets. Packets may also be lost or dropped because of a lack of resources. In most protocols, it is the responsibility of an upper- layer protocol to reorder the datagrams or ask for lost datagrams before passing them on to the application.

The datagram networks are sometimes referred to as connectionless networks. The term *connectionless* here means that the switch (packet switch) does not keep information about the connection state. There are no setup or teardown phases. Each packet is treated the same by a switch regardless of its source or destination.

Routing Table

If there are no setup or teardown phases, how are the packets routed to their destinations in a datagram network? In this type of network, each switch (or packet switch) has a routing table which is based on the destination address. The routing tables are dynamic and are updated periodically. The destination addresses and the corresponding forwarding output ports are recorded in the tables. This is different from the table of a circuit switched network in which each entry is created when the setup phase is completed and deleted when the teardown phase is over. Figure shows the routing table for a switch.



Destination address	Output port
1232	1
4150	2
.	.
9130	3

Fig 41 Routing table in a datagram network

Every packet in a datagram network carries a header that contains, among other information, the destination address of the packet. When the switch receives the packet, this destination address is examined; the routing table is consulted to find the corresponding port through which the packet should be forwarded. This address, unlike the address in a virtual-circuit-switched network, remains the same during the entire journey of the packet.

Efficiency

The efficiency of a datagram network is better than that of a circuit-switched network; resources are allocated only when there are packets to be transferred. If a source sends a packet and there is a delay of a few minutes before another packet can be sent, the resources can be reallocated during these minutes for other packets from other sources.

Delay

There may be greater delay in a datagram network than in a virtual-circuit network. Although there are no setup and teardown phases, each packet may experience a wait at a switch before it is forwarded. In addition, since not all packets in a message necessarily travel through the same switches, the delay is not uniform for the packets of a message.

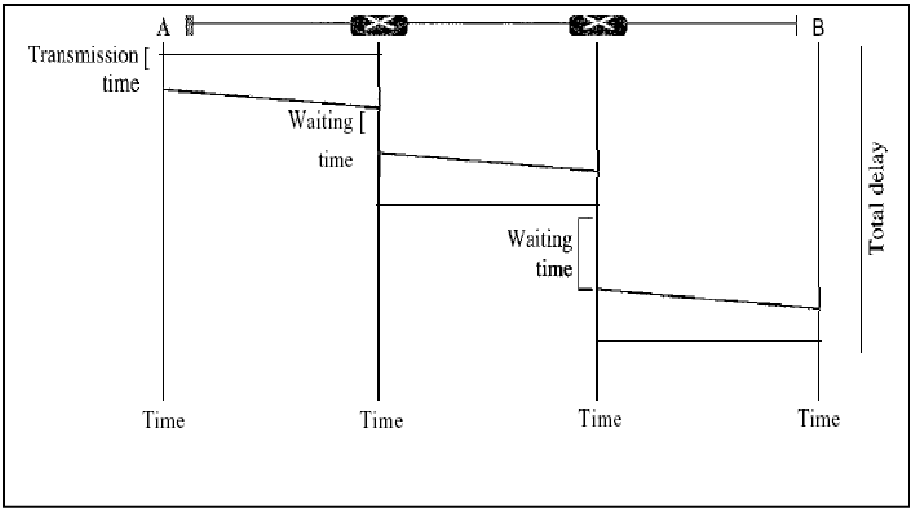


Fig 42 Delay in a datagram network

The packet travels through two switches. There are three transmission times *(3T),* three propagation delays (slopes 3't of the lines), and two waiting times (WI + *w2)'* We ignore the processing time in each switch. The total delay is
Total delay =*3T* + 3t + WI + W2

VIRTUAL-CIRCUIT NETWORKS:

A virtual-circuit network is a cross between a circuit-switched network and a datagram network. It has some characteristics of both.

1. As in a circuit-switched network, there are setup and teardown phases in addition to the data transfer phase.
2. Resources can be allocated during the setup phase, as in a circuit-switched network, or on demand, as in a datagram network.
3. As in a datagram network, data are packetized and each packet carries an address in the header. However, the address in the header has local jurisdiction (it defines what should be the next switch and the channel on which the packet is being canied), not end-to-end jurisdiction. The reader may ask how the intermediate switches know where to send the packet if there is no final destination address carried by a packet. The answer will be clear when we discuss virtual- circuit identifiers in the next section.
4. As in a circuit-switched network, all packets follow the same path established during the connection.
5. A virtual-circuit network is normally implemented in the data link layer, while a circuit- switched network is implemented in the physical layer and a datagram network in the network layer. But this may change in the future. Figure is an example of a virtual-circuit network. The network has switches that allow traffic from sources to destinations. A source or destination can be a computer, packet switch, bridge, or any other device that connects other networks.

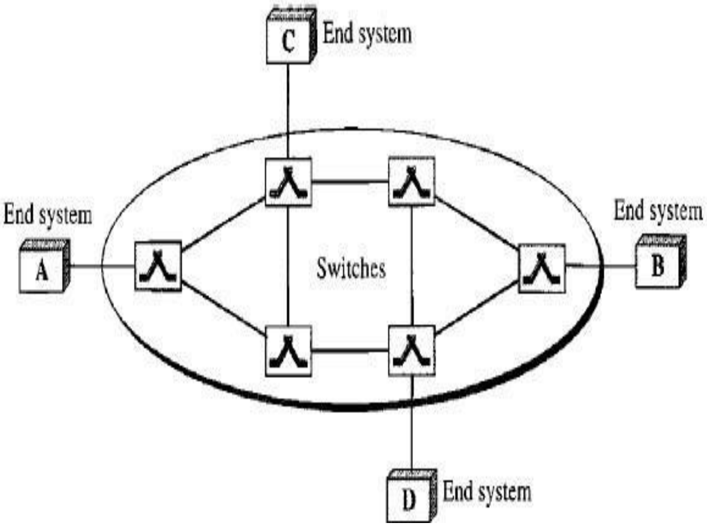


Fig 43 Virtual-circuit network Addressing

In a virtual-circuit network, two types of addressing are involved: global and local (virtual-circuit identifier).

Global Addressing*:* A source or a destination needs to have a global address-an address that can be unique in the scope of the network or internationally if the network is part of an international network. However, we will see that a global address in virtual-circuit networks is used only to create a virtual-circuit identifier, as discussed next.

Virtual-Circuit Identifier*:* The identifier that is actually used for data transfer is called the virtual- circuit identifier (Vel). A vel, unlike a global address, is a small number that has only switch scope; it is used by a frame between two switches. When a frame arrives at a switch, it has a VCI; when it leaves, it has a different VCl.

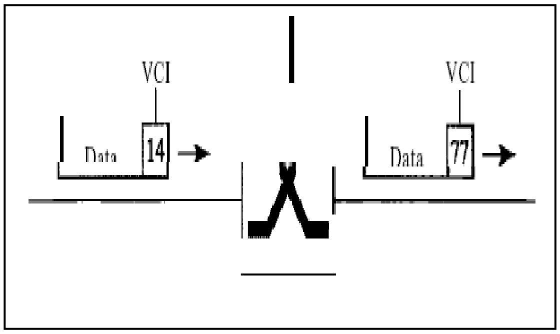


Fig 45*Virtual-circuit identifier*

Three Phases

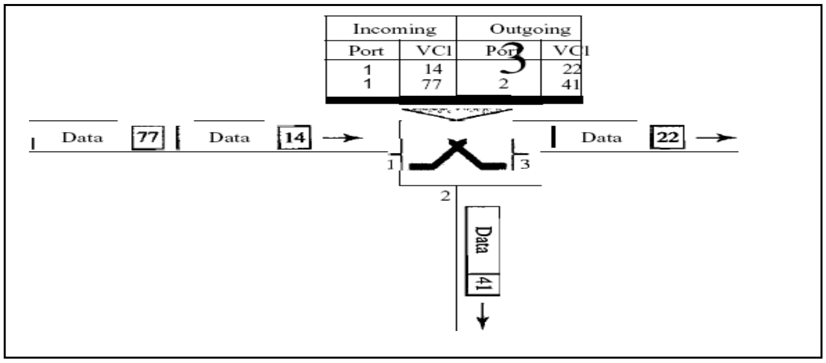
As in a circuit-switched network, a source and destination need to go through three phases in a virtual-circuit network: setup, data transfer, and teardown. In the setup phase, the source and destination use their global addresses to help switches make table entries for the connection. In the teardown phase, the source and destination inform the switches to delete the corresponding entry. Data transfer occurs between these two phases. We first discuss the data transfer phase, which is more straightforward; we then talk about the setup and teardown phases.

Data Transfer Phase

To transfer a frame from a source to its destination, all switches need to have a table entry for this virtual circuit. The table, in its simplest form, has four columns. This means that the switch holds four pieces of information for each virtual circuit that is already set up. We show later how the switches make their table entries, but for the moment we assume that each switch has a table with entries for all active virtual circuits. And also shows a frame arriving at port 1 with a VCI of 14. When the frame arrives, the switch looks in its table to find port 1 and a VCI of 14. When it is found, the switch knows to change the VCI to 22 and send out the frame from port 3. Figure shows how a frame from source A reaches destination B and how its VCI changes during the trip. Each switch changes the VCI and routes the frame. The data transfer phase is active until the source sends all its frames to the destination. The procedure at the switch is the same for each frame of a message. The process creates a virtual circuit, not a real circuit, between the source and destination.

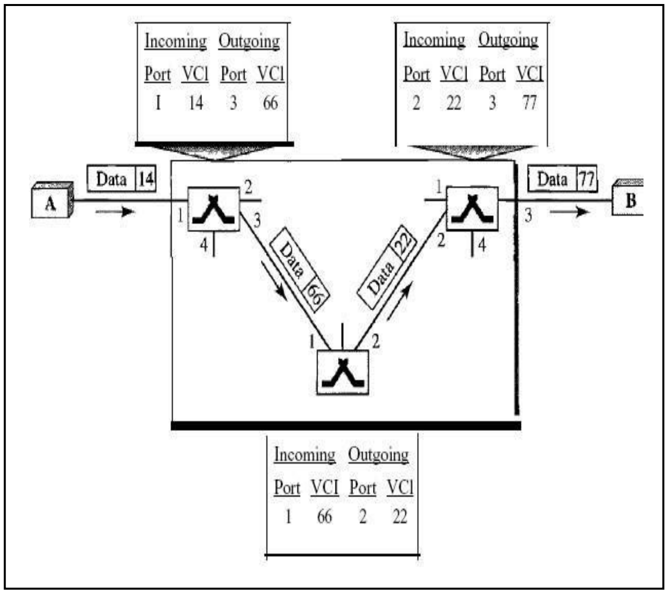
Setup Phase

In the setup phase, a switch creates an entry for a virtual circuit. For example, suppose source A needs to create a virtual circuit to B. Two steps are required: the setup request and the acknowledgment.



Incoming		Outgoing	
Port	VCI	Port	VCI
1	14	3	22
1	77	2	41

Fig 46 Switch and tables in a virtual-circuit network



Incoming		Outgoing	
Port	VCI	Port	VCI
1	14	3	66

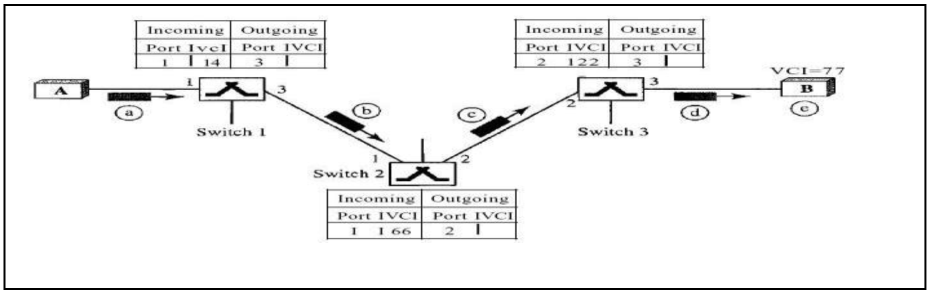
Incoming		Outgoing	
Port	VCI	Port	VCI
2	22	3	77

Incoming		Outgoing	
Port	VCI	Port	VCI
1	66	2	22

Fig 47 ***Source-to-destination data transfer in a virtual-circuit network***

Setup Request

A setup request frame is sent from the source to the destination. Figure 4 shows the process.



Incoming		Outgoing	
Port	Ivcl	Port	IVCI
1	14	3	

Incoming		Outgoing	
Port	IVCI	Port	IVCI
2	22	3	

Incoming		Outgoing	
Port	IVCI	Port	IVCI
1	66	2	

Fig 48 Setup request in a virtual-circuit network

a. Source A sends a setup frame to switch1.

b. Switch 1 receives the setup request frame. It knows that a frame going from A to B

c. goes out through port 3. How the switch has obtained this information is a point covered in future chapters. The switch, in the setup phase, acts as a packet switch; it has a routing table which is different from the switching table. For the moment, assume that it knows the output port. The switch creates an entry in its table for this virtual circuit, but it is only able to fill three of the four columns. The switch assigns the incoming port (1) and chooses an available incoming VCI (14) and the outgoing port (3). It does not yet know the outgoing VCI, which will be foundduring
the acknowledgment step. The switch then forwards the frame through port 3 to switch 2.

d. Switch 2 receives the setup request frame. The same events happen here as at switch 1; three columns of the table are completed: in this case, incoming port (l), incoming VCI (66), and outgoing port(2).

e. Switch 3 receives the setup request frame. Again, three columns are completed: incoming port (2), incoming VCI (22), and outgoing port(3).

f. Destination B receives the setup frame, and if it is ready to receive frames from A, it assigns a VCI to the incoming frames that come from A, in this case 77. This VCI lets the destination know that the frames come from A, and not other sources.

Acknowledgment A special frame, called the acknowledgment frame, completes the entries in the switching tables. The destination sends an acknowledgment to switch 3. The acknowledgment carries the global source and destination addresses so the switch knows which entry in the table is to be completed. TheframealsocarriesVCI77,chosen by the destination as the incoming VCI for frames from A. Switch 3 uses this VCI to complete the outgoing VCI column for this entry. Note that 77 is the incoming VCI for destination B, but the outgoing VCI for switch 3.

a. Switch 3 sends an acknowledgment to switch 2 that contains its incoming VCI in the table, chosen in the previous step. Switch 2 uses this as the outgoing VCI in the table.

b. Switch 2 sends an acknowledgment to switch 1 that contains its incoming VCI in the table, chosen in the previous step. Switch 1 uses this as the outgoing VCI in the table.

c. Finally switch 1 sends an acknowledgment to source A that contains its incoming VCI in the table, chosen in the previous step.

d. The source uses this as the outgoing VCI for the data frames to be sent to destination B.

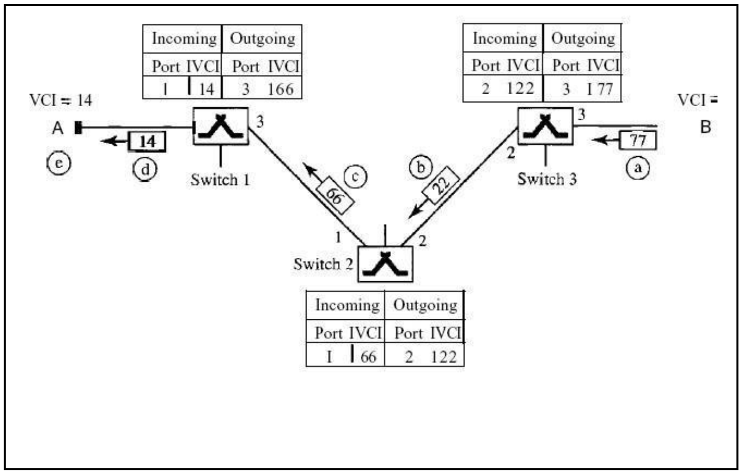


Fig 49 Setup acknowledgments in a virtual-circuit network

Teardown Phase

In this phase, source A, after sending all frames to B, sends a special frame called a *teardown request.* Destination B responds with a teardown confirmation frame. All switches delete the corresponding entry from their tables.

Efficiency

As we said before, resource reservation in a virtual-circuit network can be made during the setup or can be on demand during the data transfer phase. In the first case, the delay for each packet is the same; in the second case, each packet may encounter different delays. There is one big advantage in a virtual-circuit network even if resource allocation is on demand. The source can check the availability of the resources, without actually reserving it. Consider a family that wants to dine at a restaurant. Although the restaurant may not accept reservations (allocation of the tables is on demand), the family can call and find out the waiting time. This can save the family time and effort.

Delay in Virtual-Circuit Networks

In a virtual-circuit network, there is a one-time delay for setup and a one-time delay for teardown. If resources are allocated during the setup phase, there is no wait time for individual packets. Below Figure shows the delay for a packet traveling through two switches in a virtual- circuit network.

12. Packet Switching

Packet switching is a method of transferring the data to a network in form of packets. In order to transfer the file fast and efficient manner over the network and minimize the transmission latency, the data is broken into small pieces of variable length, called Packet. At the destination, all these small-parts (packets) has to be reassembled, belonging to the same file. A packet composes of payload and various control information. No pre-setup or reservation of resources is needed.

Packet Switching uses Store and Forward technique while switching the packets; while forwarding the packet each hop first store that packet then forward. This technique is very beneficial because packets may get discarded at any hop due to some reason. More than one path is possible between a pair of source and destination. Each packet contains Source and destination address using which they independently travel through the network. In other words, packets belonging to the same file may or may not travel through the same path. If there is congestion at some path, packets are allowed to choose different path possible over existing network.

Packet-Switched networks were designed to overcome the weaknesses of Circuit-Switched networks since circuit-switched networks were not very effective for small messages.

Advantage of Packet Switching over Circuit Switching :

- More efficient in terms of bandwidth, since the concept of reserving circuit is not there.
- Minimal transmission latency.
- More reliable as destination can detect the missing packet.
- More fault tolerant because packets may follow different path in case any link is down, Unlike Circuit Switching.
- Cost effective and comparatively cheaper to implement.

Disadvantage of Packet Switching over Circuit Switching :

- Packet Switching don't give packets in order, whereas Circuit Switching provides ordered delivery of packets because all the packets follow the same path.
- Since the packets are unordered, we need to provide sequence numbers to each packet.
- Complexity is more at each node because of the facility to follow multiple path.
- Transmission delay is more because of rerouting.
- Packet Switching is beneficial only for small messages, but for bursty data (large messages) Circuit Switching is better.

Modes of Packet Switching :

1. Connection-oriented Packet Switching (Virtual Circuit) :- Before starting the transmission, it establishes a logical path or virtual connection using signal ling protocol, between sender and receiver and all packets belongs to this flow will follow this predefined route. Virtual Circuit ID is provided by switches/routers to uniquely identify this virtual connection. Data is divided into small units and all these small units are appended with help of sequence number. Overall, three phases takes place here- Setup, data transfer and tear down phase.
All address information is only transferred during setup phase. Once the route to destination is discovered, entry is added to switching table of each intermediate node. During data transfer, packet header (local header) may contain information such as length, timestamp, sequence number etc.

Connection-oriented switching is very useful in switched WAN. Some popular protocols which use Virtual Circuit Switching approach are X.25, Frame-Relay, ATM and MPLS(Multi-Protocol Label Switching).

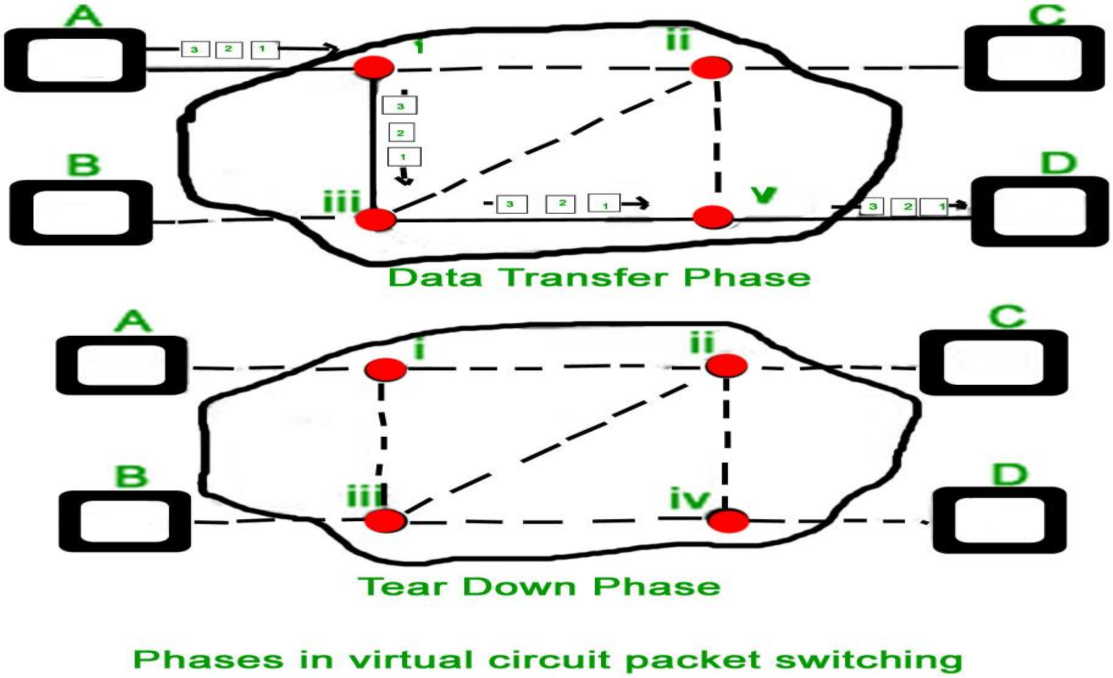


Fig 50 Packet Switching

2. Connectionless Packet Switching (Datagram) :- Unlike Connection-oriented packet switching, In Connectionless Packet Switching each packet contains all necessary addressing information such as source address, destination address and port numbers etc. In Datagram Packet Switching, each packet is treated independently. Packets belonging to one flow may take different routes because routing decisions are made dynamically, so the packets arrived at destination might be out of order. It has no connection setup and teardown phase, like Virtual Circuits.

3. Delays in Packet switching :

1. Transmission Delay
2. Propagation Delay
3. Queuing Delay
4. Processing Delay

Transmission Delay :

Time taken to put a packet onto link. In other words, it is simply time required to put data bits on the wire/communication medium. It depends on length of packet and bandwidth of network.

Transmission Delay = Data size / bandwidth = (L/B) second

Propagation delay :

Time taken by the first bit to travel from sender to receiver end of the link. In other words, it is simply the time required for bits to reach the destination from the start point. Factors on which Propagation delay depends are Distance and propagation speed.

Propagation delay = distance/transmission speed = d/s

Queuing Delay :

Queuing delay is the time a job waits in a queue until it can be executed. It depends on congestion. It is the time difference between when the packet arrived Destination and when the packet data was processed or executed. It may be caused by mainly three reasons i.e. originating switches, intermediate switches or call receiver servicing switches.

Average Queuing delay = (N-1)L/(2*R)

where N = no. of packets

L=size of packet

R=bandwidth

Processing Delay :

Processing delay is the time it takes routers to process the packet header. Processing of packets helps in detecting bit-level errors that occur during transmission of a packet to the destination. Processing delays in high-speed routers are typically on the order of microseconds or less.

13. Message Switching

Message switching was a technique developed as an alternate to circuit switching, before packet switching was introduced. In message switching, end users communicate by sending and receiving *messages* that included the entire data to be shared. Messages are the smallest individual unit.

Also, the sender and receiver are not directly connected. There are a number of intermediate nodes transfer data and ensure that the message reaches its destination. Message switched data networks are hence called hop-by-hop systems.

They provide 2 distinct and important characteristics:

1. **Store and forward –** The intermediate nodes have the responsibility of transferring the entire message to the next node. Hence, each node must have storage capacity. A message will only be delivered if the next hop and the link connecting it are both available, otherwise it'll be stored indefinitely. A store-and-forward switch forwards a message only if sufficient resources are available and the next hop is accepting data. This is called the store-and-forward property.
2. **Message delivery –** This implies wrapping the entire information in a single message and transferring it from the source to the destination node. Each message must have a header that contains the message routing information, including the source and destination.

Message switching network consists of transmission links (channels), store-and-forward switch nodes and end stations as shown in the following picture:

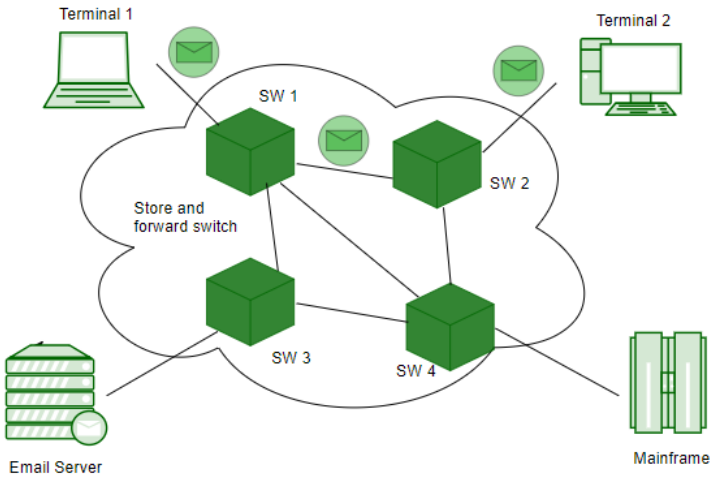


Fig 51 Message Switching

Characteristics of message switching

Message switching is advantageous as it enables efficient usage of network resources. Also, because of the store-and-forward capability of intermediary nodes, traffic can be efficiently regulated and controlled. Message delivery as one unit, rather than in pieces, is another benefit.

However, message switching has certain disadvantages as well. Since messages are stored indefinitely at each intermediate node, switches require large storage capacity. Also, these are pretty slow. This is because at each node, first there us wait till the entire message is received, then it must be stored and transmitted after processing the next node and links to it depending on availability and channel traffic. Hence, message switching cannot be used for real time or interactive applications like video conference.

Advantages of Message Switching

Message switching has the following advantages:

1. As message switching is able to store the message for which communication channel is not available, it helps in reducing the traffic congestion in network.

2. In message switching, the data channels are shared by the network devices.
3. It makes the traffic management efficient by assigning priorities to the messages.

Disadvantages of Message Switching

Message switching has the following disadvantages:

1. Message switching cannot be used for real time applications as storing of messages causes delay.
2. In message switching, message has to be stored for which every intermediate devices in the network requires a large storing capacity.

Applications

The store-and-forward method was implemented in telegraph message switching centres. Today, although many major networks and systems are packet-switched or circuit switched networks, their delivery processes can be based on message switching. For example, in most electronic mail systems the delivery process is based on message switching, while the network is in fact either circuit-switched or packet-switched.

14. Connection Oriented Services

There is a sequence of operation to be followed by the users of connection oriented service. These are:

1. Connection is established.
2. Information is sent.
3. Connection is released.

In connection oriented service we have to establish a connection before starting the communication. When connection is established, we send the message or the information and then we release the connection.

Connection oriented service is more reliable than connectionless service. We can send the message in connection oriented service if there is an error at the receivers end. Example of connection oriented is TCP (Transmission Control Protocol) protocol.

Connection Less Services

It is similar to the postal services, as it carries the full address where the message (letter) is to be carried. Each message is routed independently from source to destination. The order of message sent can be different from the order received.

In connectionless the data is transferred in one direction from source to destination without checking that destination is still there or not or if it prepared to accept the message. Authentication is not needed in this. Example of Connectionless service is UDP (User Datagram Protocol) protocol.

Difference: Connection oriented and Connectionless service

1. In connection oriented service authentication is needed, while connectionless service does not need any authentication.
2. Connection oriented protocol makes a connection and checks whether message is received or not and sends again if an error occurs, while connectionless service protocol does not guarantees a message delivery.
3. Connection oriented service is more reliable than connectionless service.
4. Connection oriented service interface is stream based and connectionless is message based.

Service Primitives

A service is formally specified by a set of primitives (operations) available to a user process to access the service. These primitives tell the service to perform some action or report on an action taken by a peer entity. If the protocol stack is located in the operating system, as it often is, the primitives are normally system calls. These calls cause a trap to kernel mode, which then turns control of the machine over to the operating system to send the necessary packets. The set of primitives available depends on the nature of the service being provided. The primitives for connection-oriented service are different from those of connection-less service. There are five types of service primitives :

1. **LISTEN :** When a server is ready to accept an incoming connection it executes the LISTEN primitive. It blocks waiting for an incoming connection.
2. **CONNECT :** It connects the server by establishing a connection. Response is awaited.
3. **RECIEVE:** Then the RECIEVE call blocks the server.
4. **SEND :** Then the client executes SEND primitive to transmit its request followed by the execution of RECIEVE to get the reply. Send the message.
5. **DISCONNECT :** This primitive is used for terminating the connection. After this primitive one can't send any message. When the client sends DISCONNECT packet then the server also sends the DISCONNECT packet to acknowledge the client. When the server package is received by client then the process is terminated.

Connection Oriented Service Primitives

There are 5 types of primitives for Connection Oriented Service :

LISTEN	Block waiting for an incoming connection
CONNECTION	Establish a connection with a waiting peer
RECEIVE	Block waiting for an incoming message
SEND	Sending a message to the peer
DISCONNECT	Terminate a connection

Connectionless Service Primitives

There are 4 types of primitives for Connectionless Oriented Service:

UNIDATA	This primitive sends a packet of data
FACILITY, REPORT	Primitive for enquiring about the performance of the network, like delivery statistics.

SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited “A” Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

School of Computing

Department of Computer Science and Engineering

UNIT - IV

Data Communication and Computer Networks- SBS1302

History of Analog and Digital Network - Access to ISDN - ISDN Layers – Broadband ISDN X.25 Layers - Packet Layer Protocol - ATM - ATM Technology - ATM protocol.

1. History:

Voice Communication over analog n/ws:

Initially, telecommunication n/ws were entirely analog n/ws and were used for the transmission of analog information in the form of voice. Local loops connecting the subscriber's handset to the telephone company's central office were also analog.

Voice and data communication over Analog n/ws:

With the advent of digital processing, subscribers needed to exchange data as well as voice.Modems, developed to allow digital exchanges over existing analog lines.

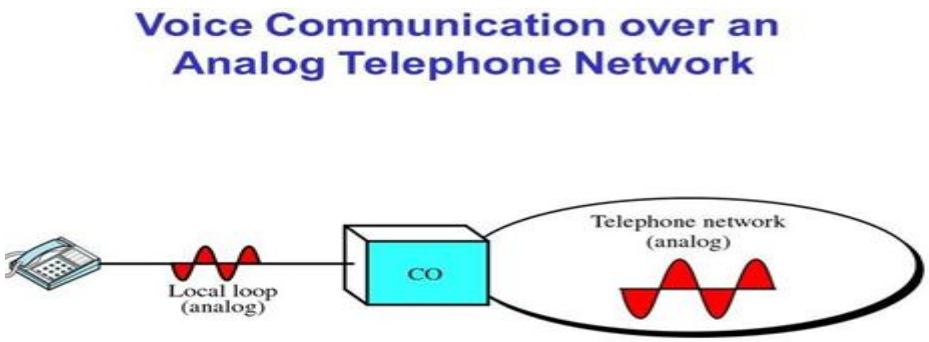


Fig 1 Voice Communication over an Analog Telephone Network

Analog and digital services to subscribers:

Three types of customers: Traditional Customers using their land loops only for analog purposes, customers suing analog facilities to transmit digital information via modem, customers using digital services to transmit data i.e. digital information.First group was prominent, so most services offered remainedanalog.

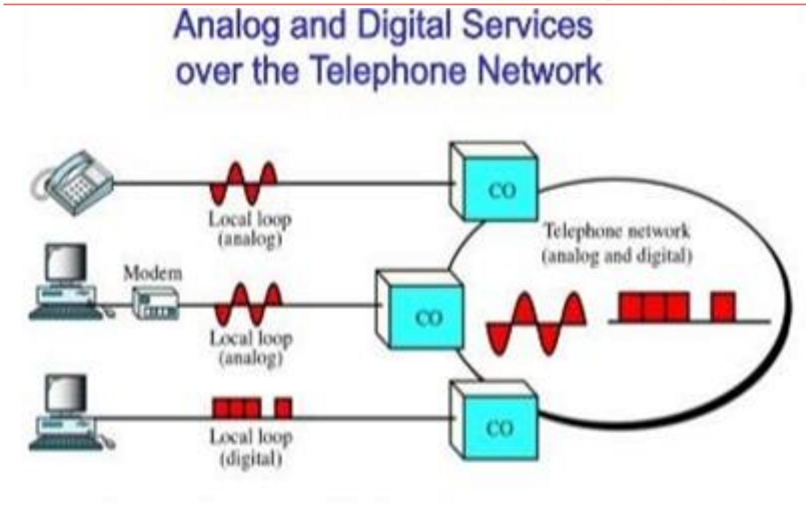


Fig 2 Different Types of Customers

2. ISDN

Integrated Digital N/w (1DN):

Customers needed access to variety of N/ws, such as packet switched n/ws and circuit switched n/ws, so telephone companies created 1DNs.An IDN is a combination of n/ws available for different purposes.Access to these n/ws is by digital pipes, which are time-multiplexed channels sharing very high speed paths.

ISDN integrates customer services with the IDN. With ISDN all customer services will become digital rather than analog and the flexibility offered by the new technology will allow customers services to be made available on demand. ISDN incorporates all communications connections in a home or building into a single interface.

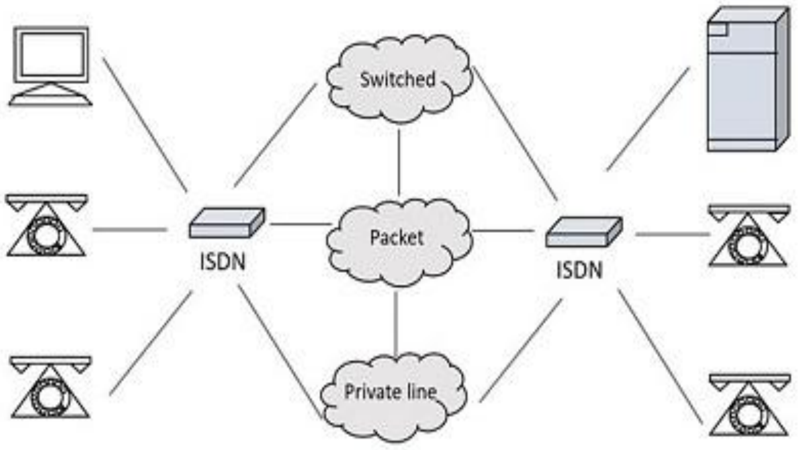


Fig 3 ISDN Architecture

ISDN Applications

- Voice calls
- Facsimile
- Videotext
- Tele text
- Electronic Mail
- Database access
- Data transmission and voice
- Connection to internet
- Electronic Fund transfer
- Image and graphics exchange
- Document storage and transfer

Subscriber Access to the ISDN:

ISDN standard defines 3 channel types, each with a different transmission rate: bearer channels, data channels and hybrid channels.

B Channels:

A bearer channel defined at a rate of 64kbps.It is a basic user channel and can carry any

type of digital information in full duplex mode.B – Channel carries transmissions end to end.

D Channels:

A data channel can be either 16 or 64 kbps, depending on the needs of user.Primary function is to carry control signaling for the B channels, using a method called common channel (out of band) signaling. D channel acts like an operator between the user and the n/w at the n/w layer. Less common uses for D channel include low rate data transfer and applications such as telemetry and alarm transmission.

H Channels:

Hybrid channels are available with data rates of 384 Kbps (HO), 1536 K6ps (H11), or 1920 Kbps(H12).These rates suit H channels for high data rate applications such as video, tele-conferencing etc.

User Interfaces:

Digital subscriber loops are of 2 types: basic rate interface (BRI) and primary rate interface(PRI).Both include one D channel and some number of either B or H channels.

BRI:

It specifies a digital pipe consisting of 2 B channels and one 16 K6ps D channel.2 B channels of 64 K6ps each, plus 1 D channel of 16 K6ps, equals 144K6ps.Additionally, BRI itself requires 48 K6ps of operating overhead. Therefore, requires a digital pipe of 192K6ps.

BRI service is like a large pipe with 3 smaller pipes, remainder of space inside the large pipe carries the overhead bits required for its operation.BRI is designed to meet the needs of residential & small office customers. Same twisted pair local loop that delivers analog transmission can be used to handle digital transmission.

PRI:

It specifies a digital pipe with 23 B channels & one 64 Kbps D channel.23 B channels of 64Kbps each ,plus 1D channelof64K6ps,equals1.536 Mbps. Additionally, PRI itself uses 8 Kbps of overhead. digital pipe of 1.544 Mbps. So PRI is a large pipe with 24 smaller pipes,

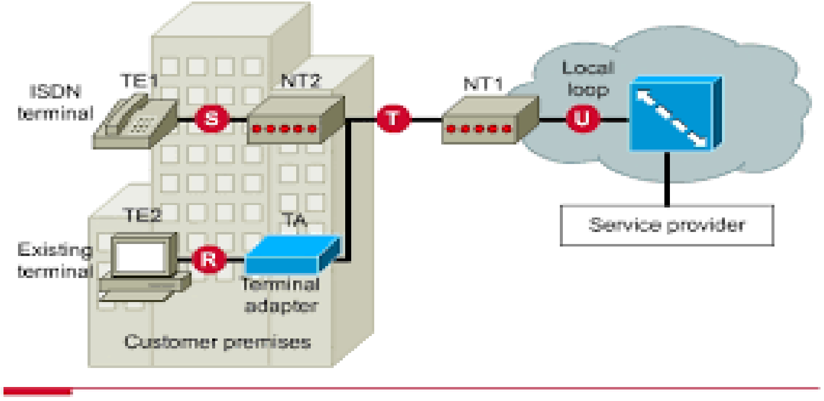
23 for B & 1 for D channels. Rest of the pipe carries the overhead bits required for its operation. The individual transmissions are collected from their sources & multiplexed onto a single path for sending to the ISDN office. For more specialized transmission needs, other channel combinations are also supported by PRI standard. They are 3HO+D, 4HO+D & H12+D.

Functional Grouping:

In ISND standard, the devices that enable users to access the services of the BRI or PRI are described by their functional duties and collected in functional grouping. Each functional grouping is a model that can be implemented using devices or equipment chosen by thesubscriber. Functional groupings used are n/w terminations (types 1&2) terminal equipment (types 1 & 2) terminal adapters.

N/w Termination 1(NT10:

An NT1 device controls the physical & electrical termination of the ISDN at the users premises and connects the users internal system to the digital subscriber loop.An NT1 organizes the data streams from a connected subscriber into frames that can be sent over the digital pipe, and translates the frames received from the n/w into a format usable by the subscriber's devices. An NT1 synchronizes the data stream with the frame – building process in such a way that multiplexing occurs automatically.



• Functions refer to devices or hardware functions

Fig 4 N/W Termination Device

N/W Termination 2(NT2)

An NT2 device performs functions at the physical, data link & n/w layers of the OSI model (layers 1,2&3).NT2s provide multiplexing (layer1), flow control (layer 2) & packetizing (layer3).An NT2 provides intermediate signal processing between the data- generating devices and anNT1.NT2s can be implemented by a variety of equipment types. eg. a private branch exchange (digital PBX) can be an NT2 – it coordinates transmissions from a number of incoming links (user phone lines) and multiplexes them to make them transmittable by anNT1.A LAN also can function as anNT2.

Terminal Equipment 1(TE1):

The term terminal equipment is used by ISDN std. to mean the same thing as DTE in other protocols. It refers to digital subscriberequipment.TE1 is any device that supports the ISDN stds. Egs. Digital telephones, integrated voice / data terminals & digital facsimiles.

Terminal Equipment 2(TE2):

To provide backward compatibility with a customer's existing equipment, the ISDN std. defines a second level of terminal equipment calledTE2.TE2 is any non – ISDN device, such as terminal, workstation, host computer or regulartelephone.TE2 devices are not immediately compatible with an ISDN n/w but can be used with the help of another device called a terminal adapter (TA).

Terminal Adapter(TA):

TA converts information received in non- ISDN format from a TE2 into a format capable of being carried by the ISDN.

Reference points:

Here, reference points refer to the label used to identify individual interfaces between 2 elements of an ISDN installation. Functional grouping defines the function of each types of equipment used in ISDN, reference points defines the functions of the connections between them. Specifically, a reference point defines how 2 n/w elements must be connected and the format of the traffic between them.

Reference point R defines the connection between a TE2 & a TA; Reference point S defines the connection between a TE1 or TA & an NT1 or NT2 (if present); Reference point T defines the interface between an NT2 & an NT1; Reference point U defines the interface between an NT1 and the ISDN office.

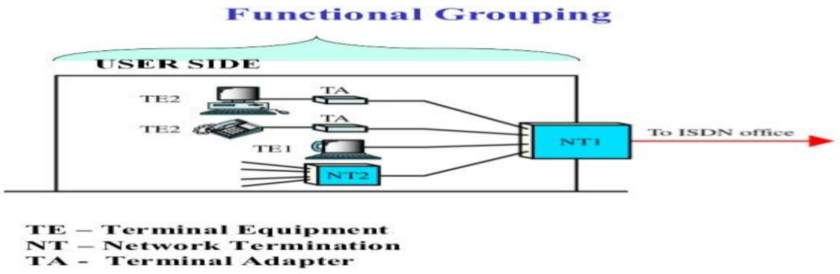


Fig 5 TE1 and TE2

3. ISDN layers:

The ITU-T has devised an expanded model for the ISDN layers.Instead of a single 7 layer architecture like the OSI, the ISDN is defined in the three separate planes: the user plane, the control plane and the management plane.All 3 planes divided into 7 layers that correspond to the OSI model.

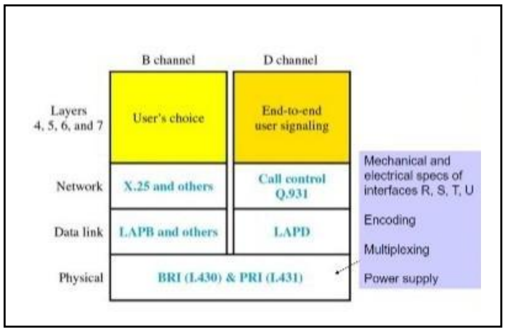


Fig 6 ISDN Layers

Physical layer:

TheISDNphysicallayerspecificationsaredefinedby2ITU-Tstds.I.430 for BRI access and I. 431 for PRI access. These stds. define all aspects of the BRI and PRI. Of these 4 are important. The mechanical & electrical specifications of interfaces R,S,T&U Encoding. Multiplexing channels to make them carriable by the BRI& PRI digital pipes power supply.

Physical layer specifications forBRI:

BRI consists of 2B channels & one D channel. A subscriber connects to the BRI using the R, S, & U interfaces (reference points).

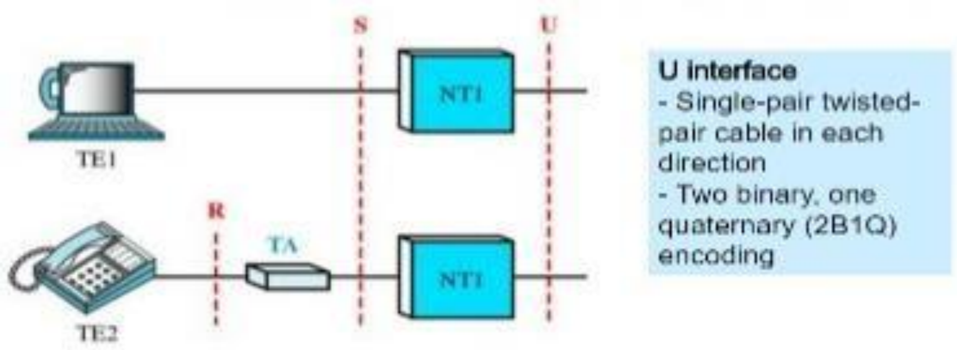

S
U
NT1
TE1
R
TA
NT1
TE2
U interface
- Single-pair twisted-pair cable in each direction
- Two binary, one quaternary (2B1Q) encoding

Fig 7 Interfaces

R interface:

This interface not defined by the ISDN.A subscriber can use any of the EIA stds (such as E1A-232, E1A-499, or E1A-530) or any of the V or X series standards (such as x.21).

S interface:

For S interface, ITU-T specifies the ISO std.ISO8887.This std. calls for four -, six-, or eight wire connections.The signal used in the s interface is pseudo ternary encoding.

U-interface:

For U interface (digital subscriber or local loop), the ITU –T specifies a single pair twisted – pair cable in each direction. Encoding for this interface uses a method called two binary, one quaternary(2B1Q).2B1Q uses 4 voltage levels instead of two.The 4 voltage levels represent the bits 00, 01, 10 &11.

BRI frame:

Each B channel is sampled twice during each frame (8 bits per sample).The D channel is sampled four times during each frame (one bit per sample).The entire frame consists of 48 bits : 32 bits for the B Channels, 4 bits for the D channel, & 12 bits of overhead.

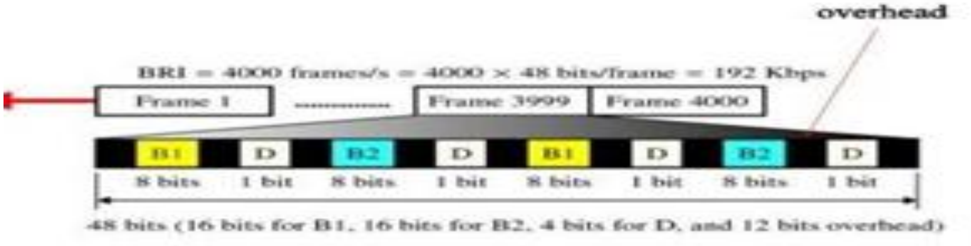

overhead
BRI = 4000 frames/s = 4000 × 48 bits/frame = 192 Kbps
Frame 1
....
Frame 3999
Frame 4000
B1
D
B2
D
B1
D
B2
D
8 bits
1 bit
8 bits
1 bit
8 bits
1 bit
8 bits
1 bit
48 bits (16 bits for B1, 16 bits for B2, 4 bits for D, and 12 bits overhead)

Fig 8 BRI Frame

Connection andTopology:

BRI services can be supported by either a bus or star topology.The main restriction governing the choice of topology for a BRI is the distance of the data devices from theNT1.In a point to point connection, each device can be as far as 1000 meters away from theNT1.In a multipoint connection, the maximum length of the line generally cannot be more than 200meters.

This restriction is necessary to ensure frame synchronization.If the synchronization between the frame and the devices is off, data dumped by one device can end up in a part of the frame devoted to data from another device, or to another kind of informational together.Unavoidable propagation delays over distance can result in a shifted frame.

IF the distance between the first and the last device on a link is great enough, data collection timing can deteriorate the frame.Clustering the devices means that propagation delays will impact the data from all devices almost equally, allowing the relationship between the data units to remain predictable for 500meters.As many as 8 devices can be connected to anNT1.Of these, only 2 can access the B channels at one time, one exchange perchannel.Every device, however can contend for access tot eh Dchannel.D Channels use a mechanism like CSMA to control access.Once device has access to D channel, it can request a B channel.If B channel is available, the connection is made by the D channel and the user may then send data.

Physical layer specifications for PRI:

The PRI consists of 23B channels and 1 D channel. Interfaces associated with PRI usage include R.S.T. &U. The R&Sstds. are the same as those defined for the BRI. The T std. is identical to S Std. with the substitution of B8ZS encoding.TheUinterfaceisthesameforbothstds.exceptthatthePRIrateis1.544 Mbps instead of 192 Kbps: 1.544 Mbps allows the PRI to be implemented using T-1 specifications.

PRI frame:

The B and D channels are multiplexed using synchronous TDM to create a PRI frame.

The frame formats identical to that defined for T-1lines.PRI frame samples each channel, including the D channel, only once perframe.

Connection and Topology

Can be the same as those described for the device to NT1 links in the BRI, or they can differ (depends on application).The link from NT2 to NT1 must always be point topoint.If NT2 is LAN, its topology will be specified by LAN being used, If NT2 is a PBX, its topology will be specified by the PBX being used & soon.

Data Link Layer:

B and D channels use different data link protocols, B channels use LAPB protect. The D channel uses link access procedure for D channel(LAPD).First, LAPD can be used in either unacknowledged (without sequence numbering) or acknowledged (with sequence numbering)formats. The unacknowledged format is used only seldomly.

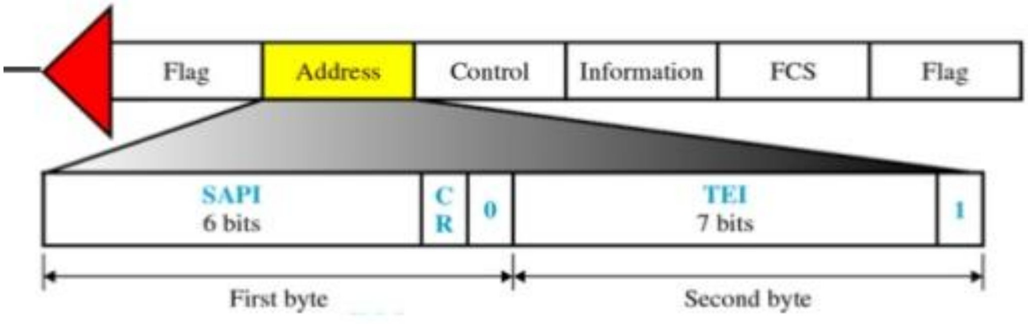


Fig 9 Data Link Layer Packet Format

LAPD addressing:

The address field of the LAPD is 2 bytes long. The first byte contains a b – bit field called a service access point identifier (SAP1) a 1-bit command / response field set to 0 if the frame is a command and to 1 if the frame is a response I and a 1 bit field set to 0 to indicate that the address is continued in the next byte .The 2nd byte contains a 7 bit field called a terminal equipment identifier (TEI) and a one – bit field set to 1 to indicate that the address is complete.

SAPI field:

Identifies the type of upper – layer service (n/w layer) using the frame.It indicates the intended use of the D channel.It is a 6 – bit field and can therefore define up to 64 different service access points.To date, only 4 of the possible bit combinations have been assigned.
000000- Call control for n/w layer (signaling use of D channel)
000001-Call control for upper layer (end to end signaling),not yet in use.

010000- Packet communication (data use of D channel).

111111 - Management.

TE1field:

The TE1 field is the unique address of the TE.It consists of 7 bits and can therefore identify upto128 different TEs.

Network Layer:

Once a connection has been established by the D channel, the B Channel sends data using circuit switching, x .25, or other similar protocols. The functions are defined by the ITU-T Q. 931standard.The network layer packet is called a message. A message is encapsulated in the information field of an LAPD I frame for transport across a link.

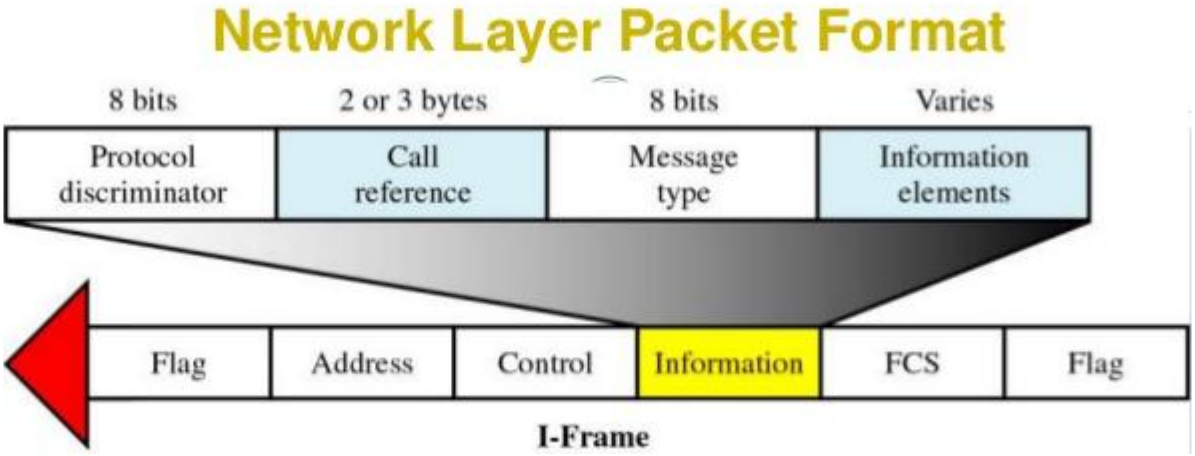


Fig 10 Network Layer Packet Format

The format of the message have 4fields:

- Protocol discrimination (a single one byte field).
- Call reference (2-or3 byte field)
- Message type (a single one byte field)
- Information elements (a variable number of variable length fields).

Protocol discriminator:

This field identifies the protocol in use. For Q. 931, the value of this field is00001000.

Call Reference:

It is the sequence number of the call. The format is shown infigure.

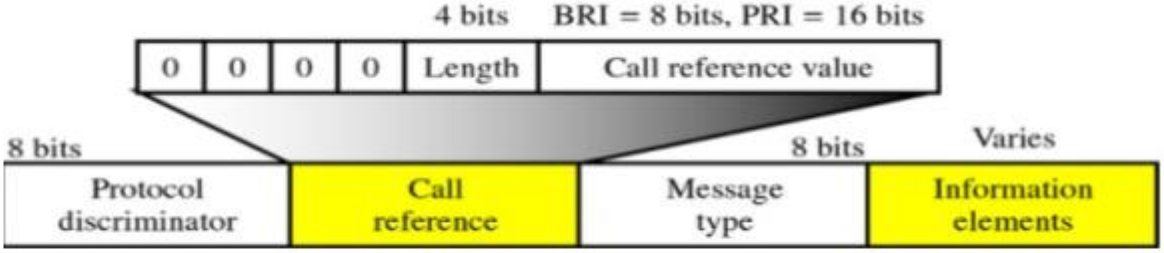


Fig 11 Call Reference Field

Message Type:

It is a one byte field that identifies the purpose of the message.

4 categories of message types: call establishment messages, call information messages, call clearing messages, & miscellaneous messages.

Call Establishment Message:

- Setup – sent by the calling user to the n/w or by the n/w to the called user to initiate a call.
- Setup Acknolwedgement – sent by called user to n/w or by n/w to calling user to indicate that setup has been received (no connection).
- Connect – sent by called user to n/w or by n/w to calling user to indicate acceptance of the call.
- Connect acknowledgement – sent by the n/w to the called user to say that the desired connection has been awarded.
- Progress – sent by n/w to called user to indicate that call establishment is in progress.
- Alerting – sent by the called user to n/w or by n/w to calling user to indicate that the call user alert (ringing) has been initiated.
- Call Processing – sent by called user to n/w or by n/w to the calling user to indicate that the requested call establishment has been initiated and that no more information is needed.

Call Information Message:

- Resume – sent by a user to the n/w to request that a responded call be resumed.
- Resume Acknowledgement – sent by the n/w to the user to acknowledge a request to resume the call.
- Suspend – sent by a user to request that the n/w suspend a call.
- Suspend acknowledgement – sent by n/w to user to acknowledge the requested

suspension of the call.

- Suspend reject – sent by n/w to user to reject the requested suspension.
- User Information – sent by user to n/w to be delivered to the remote user.

Call Clearing Messages:

- Disconnect – sent by the called user to the n/w or by the n/w to the called user to clear the end to end connection(termination).
- Release – sent by a user or n/w to indicate the intention to disconnect and release the channel.
- Release complete – sent by a user or n/w to show that the channel has been released.
- Miscellaneous – other messages carry information defined in the protocols of specific services.

Information Elements:

An information elements field carries specific details about the connection that are required for call establishment.

Information Element types:

An information element consists of one or more bytes.A one byte information element can be of type 1 or type2.In type 1, the 1st bit is 0, the next 3 bits identify the information being sent, and the remaining 4 bits carry the specific content or attribute of the element. Type 2 elements start with a 1 bit, the remainder of the bit reserved for the ID.In multi byte information element, the 1st bit of the 1st byte is 0 and the remainder of the byte is the ID. The 2nd byte defines the length of the content in bytes, the remaining bytes are content.

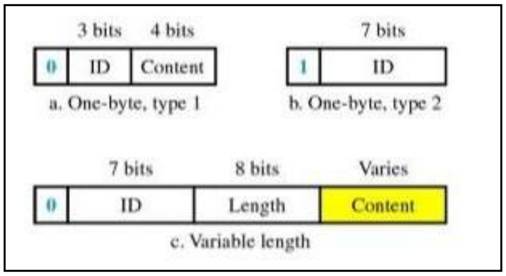
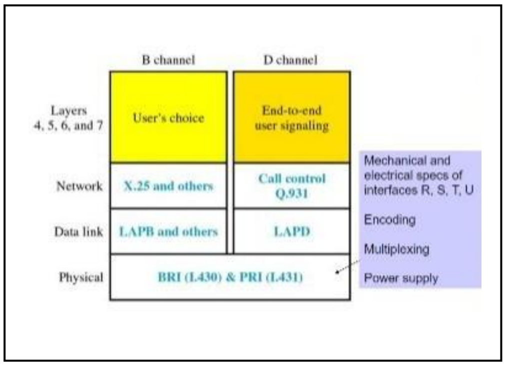


Fig 12 Information Element Types

Addressing:

An important type of information element is addressing.The country code consists of 3digits.The NC field is the national code and consists of 2digits.It identifies the specific n/w in countries with more than one ISDN n/w. The subscriber number is the 10 digit number familiar from national telephone numbers; a 3 digit area code & a 7 digit phone number.



together these, 15 digits define the access to a subscriberNT1.An NT1 may have multiple devices connected to it, either directly or indirectly through anNT2.Each device is identified by a sub-address.The ISDN allows up to 40 digits for a sub-address.

4. Broadband ISDN:

When the ISDN was originally designed, data rates of 64 kbps to 1.544 Mbps were sufficient to handle all existing transmission needs.As applications using the telecommunications n/ws advanced, these rates proved inadequate to support many applications. In addition, the original bandwidths proved too narrow to carry the large numbers of concurrent signals produced by a growing industry of digital service providers.

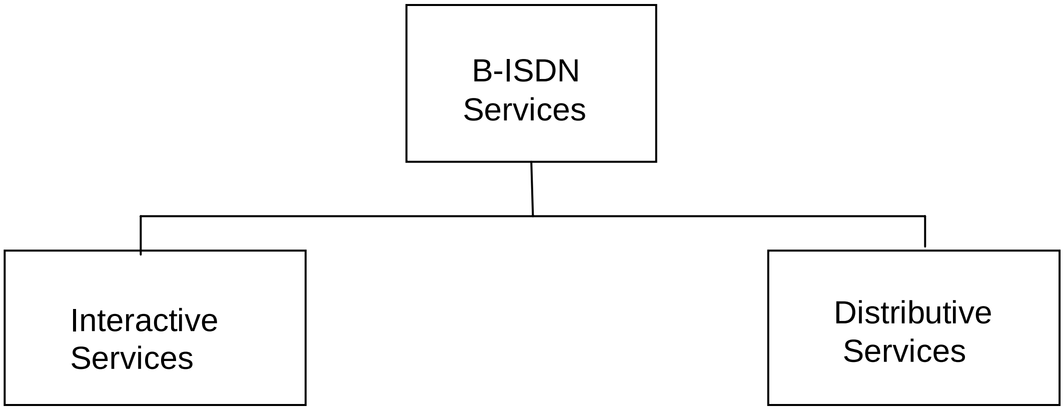
To provide the needs for next generation technology, an extension of ISDN called Broadband ISDN (B-ISDN) is understudy. The original ISDN is now known as narrow band ISDN(N-ISDN).B-ISDN provides subscribers to the n/w with data rates in the range of 600 mbps, almost 400 times faster than the PRI rate.B-ISDN not yet implemented or standardized. B-ISDN is based on a change from metal cable to fiber – optic cable at all levels of tele-communications.

Services:

B-ISDN provides 2 types of services interactive &distributive.

Interactive Services:

Interactive services are those that required two – way exchange between either two subscribers or between a subscriber and a service provider.



These services are of 3 types : conversational, managing &retrieval.

Conversational:

Conversational services are those, such as telephone calls, that support real – time exchanges. These real time services can be used for telephony, video telephony, video conferencing, data transfer, and soon.

Messaging:

Messaging services are store- and forward exchanges.These services are bidirectional, meaning that all parties in an exchange can use them at the same time. The actual exchange, may not occur in real time.One subscriber asking another for information may have to wait for an answer, even though both parties are available at the same time.These services include voice mail, data mail and video mail.

Retrieval:

Retrieval services are those used to retrieve information from a central source, called an information centre. These services are like libraries: they must allow public access and allow users to retrieve information ondemand.eg. A videotext that allows subscribers to select video data from an online library.Service is bidirectional because it requires action on the part of both the requester and the provider.

Distributor Services:

These are unidirectional services sent from a provider to subscribers without the subscriber having to transmit a request each time a service is desired.These services can be without or with user control.

Without user control:

These services are broadcast to the user without the user's having requested them or having control over either broadcast times or content. User choice limited to whether or not to receive the service at all. eg. commercial TV – programming content & times devided by provider alone.

With user control:

These services are broadcast tot eh user in a round – robin fashion.Services are repeated periodically to allow the user a choice of times during which to receive them Which services are broadcast at which times, is the option of the provide alone.With pay TV a program is made available in a limited number of time slots. A user wishing to view the program must activate his or her television to receive it, but he or she has no other control.

Physical Specifications:

B- ISDN model is divided into layers that are different from N- ISDN and closely tied to the design of ATM.Physical aspects of B-ISDN not related to ATM include access methods, functional equipment groupings and reference points.

Access Methods:

B-ISDN defines 3 access methods designed to provide for 3 levels of user needs.

155.520 Mbps full duplex:

This rate matches that of an OC – 3 Sonetlink.It is high enough to support customers who need access to all N-ISDN services and to one or more regular video transmission services. This method is geared to fill the needs of most residential and many business subscribers.

155.520 Mbps output / 622.080 Mbps input:

The outgoing rate is 155.520 Mbps (same as an OC – 3 Sonet Link), but the incoming rate is 622.080 Mbps (same as an Oc-12 sonetlink).Designed to fill the needs of business that require the simultaneous receipt of multiple services and video conferencing but that are not service providers & don not broadcast distributive services.Input needs of these subscribers are far greater than their o/p needs. Providing only one rate would either limit their receipt of services or result in wasted link capacity. The asymmetrical configuration provides for a balanced use of resources.

622.080 Mbps full duplex:

This is designed for business that provide and receive distributive services.

Functional Grouping:

The functional groupings of equipment in the B-ISDN model are same as those forN-ISDN.Here they are called B-NT1, B-NT2, B-TE1, B-TE2 andB-TA.

Reference Points:

B-ISDN uses the same reference points as N-ISDN (R, S, T, & U); some of these, are currently under scrutiny and may bere defined.

Future of Isdn:

The N-ISDN was designed to replace the analog telephone system with a digital one for both voice and data transmission.

N-ISDN has replaced the normal telephone line in some European countries but in United States this replacement was delayed and new technologies such as cable modem and ADSL evolved that make N- ISDN questionable.However ISDN can still be considered a good solution for several reasons:

- First SIDN can be brought to a subscriber premise with minimum cost and the services available can satisfy the needs of many users.
- Second, new equipment has appeared on the market that allows a subscriber to use the entire bandwidth of an ISDN link (192 Kbps for BRI or 1.544 Mbps for PRI)
- Third, the protocol is flexible enough to be upgraded to higher data rates using new technology and new transmission media.
- Fourth, N-ISDN can be used as a fore runner for B-ISDN, the data rate of which is sufficient for several years to come.

5. Packet Layer ProtocolX.25

It is a Packet-Switching wide are a network.It is an interface between Data Terminal Equipment(DTE) and Data- Circuit terminating Equipment(DCE). It describes the procedures for data transmission between a DTE and a DCE for terminal operation in the packet mode on public data networks.It is also known as Subscriber Network Interface(SNI) protocol.It uses VC approach to packet switching(SVC and PVC) and uses asynchronous(statistical) TDM to multiplex packet

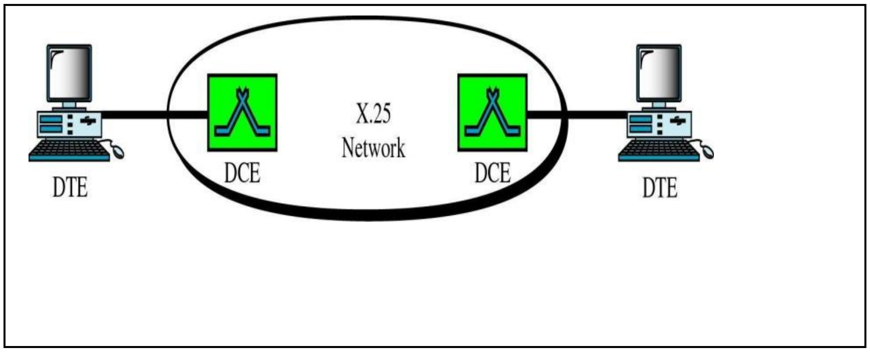


Fig 14 X.25 Protocol

X.25Layers

The three layers are Physical , frame (data link) and packet (network) layer.Physical layer specifies X.21 protocol. At frame layer X.25 provides data link control using a bit-oriented protocol called Link Access Procedure ,Balanced(LAPB).

X.25 Layers in Relation to the OSILayers

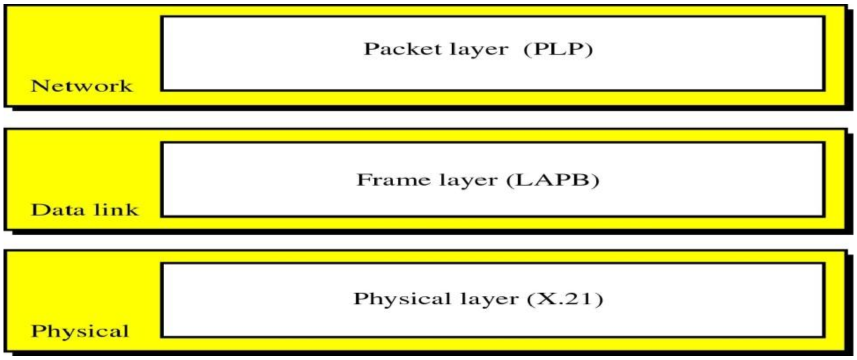


Fig 15 Layers of X.25

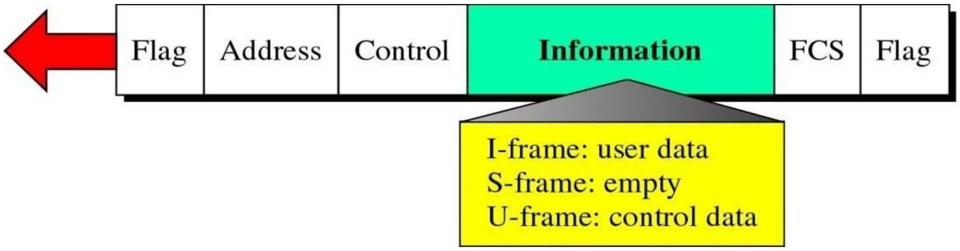


Fig 16 Frame Format

I – Frames are used o encapsulate PLP packets from the network layer

S – Frames are for flow and error control in the frame layer.

U – Frames are used to set up and disconnect the links between a DTE and aDCE

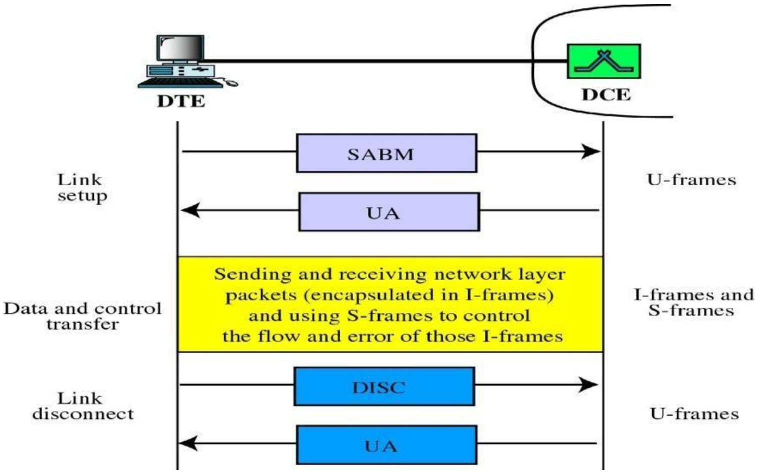
Three Phases of the Frame Layer

- **Link Setup** – The link between DTE and DCE must be setup before packets are transferred. Either DTE or DCE can setup the link by sending a SABM(Set Asynchronous Balanced Mode) frame, the responding party sends an UA(Unnumbered Acknowledgement)frame.

- **Data Transfer** – after the link has been established the two parties can send and receive network layer packets using I – frames and S –frames.

- **Link Disconnect** – When the network no longer needs the link, one of the parties issue a Disconnect(DISC) frame and other party replies with an UA frame.

Fig 17 Phases of Frame Layer


DTE
DCE
SABM
Link setup
U-frames
UA
Sending and receiving network layer packets (encapsulated in I-frames) and using S-frames to control the flow and error of those I-frames
Data and control transfer
I-frames and S-frames
DISC
Link disconnect
U-frames
UA

Packet Layer

Packet Layer handles connection establishment, data transfer, connection termination , Virtual Circuit creation and negotiation of network services between twoDTEs.Frame layer is responsible for connection between DTE and DCE, whereas packet layer is responsible for making connection between two DTE's.X.25 uses flow and error control at both frame and packetlayer.

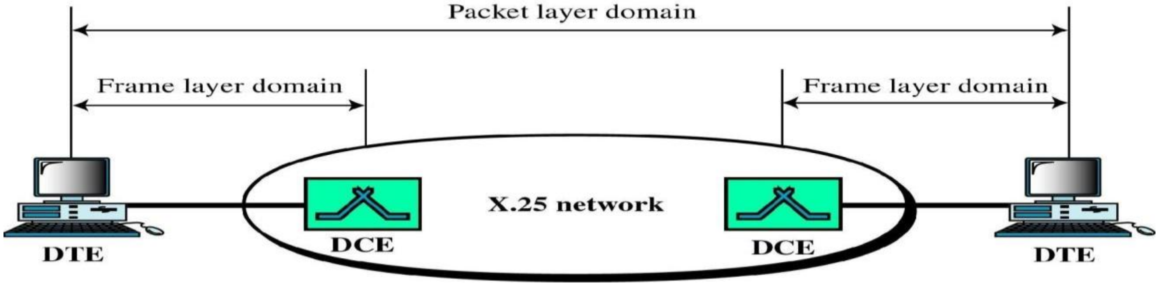


Fig 18 Packet Layer Communication

Virtual Circuit Identifiers

Virtual circuit identifier in X.25 is called the Logical Channel Number(LCN). When VC is established there is always a pair of LCNs. One defining the VC between the local DTE and local DCE and the other one between DCE and remote DTE.

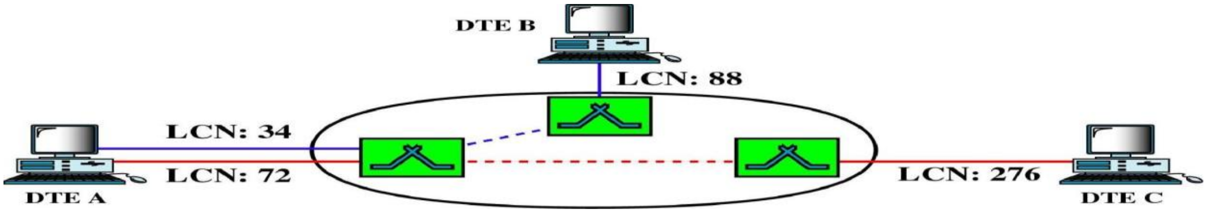


Fig 19 Virtual Circuit Identifiers

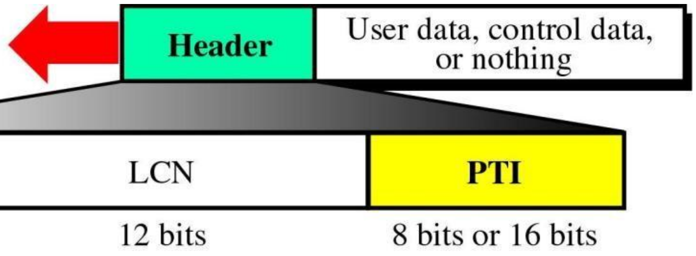


Fig 20 Packet Structure

- **General Format identifier(GFI)**
- **Logical Channel Number(LCN)**
- **Packet Type Identifier(PTI)**

Categories of PLP Packets

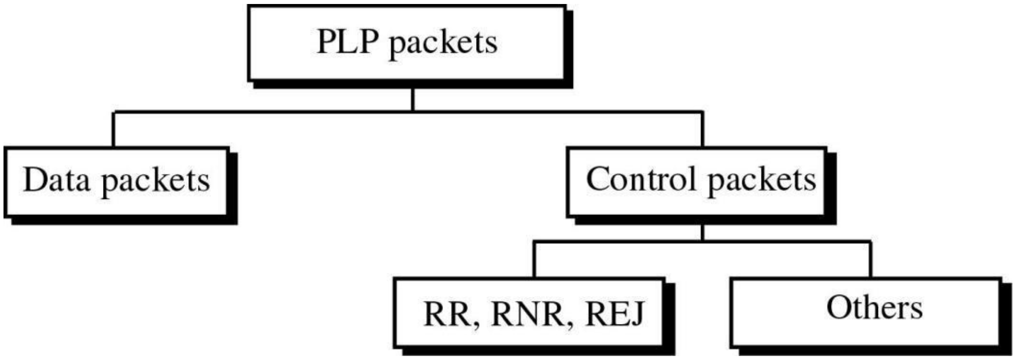
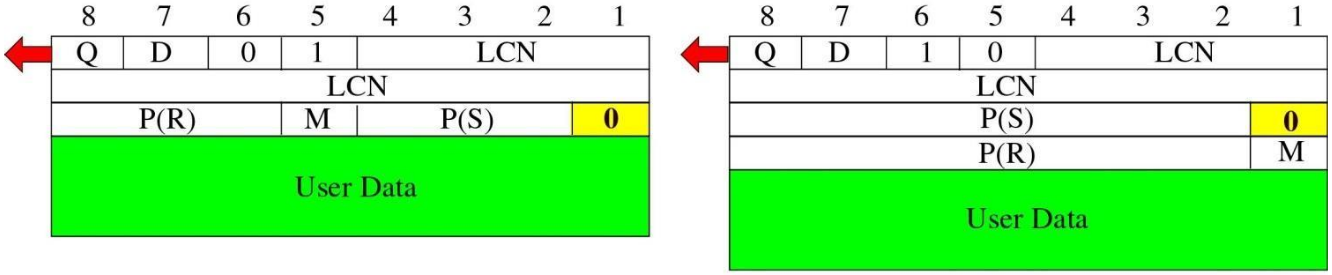


Fig 21 Data Packets in the PLP Layer



a. Three-bit sequence number

b. Seven-bit sequence number

Fig 22 a)Three bit sequence number b) Seven bit sequence number

6. ATM

Asynchronous Transfer mode (ATM) is the cell relay protocol designed by the ATM Forum and adopted by ITU-T. The combination of ATM and B-ISDN will allow high speed interconnection of all the world's network.

ATM Architecture:

ATM is a cell – switched n/w.The user access devices, called the end points are connected through a user to network interface (UNI) to the switches inside the network. The switches are connected through network to network interfere(NNIs).

ATM Architecture

- UNI: user-to-network interface
- NNI: network-to-network interface

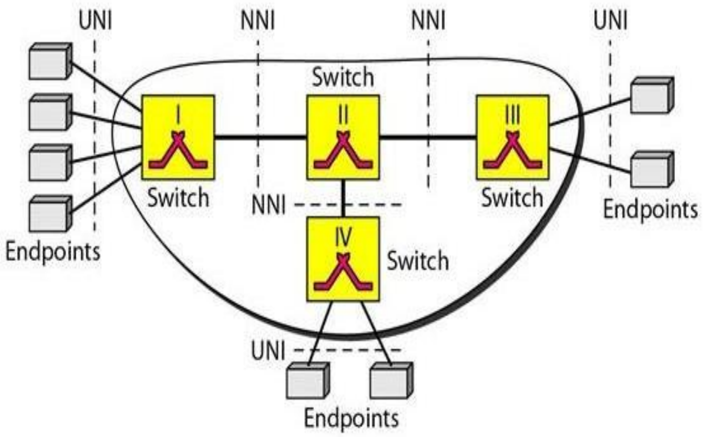


Fig 23 ATM Architecture

Virtual Connection:

A Transmission path (TP) is the physical connection (wire, cable, satellite, etc.) between an end point and a switch or between two switches. A transmission path is divided into several virtual paths. A virtual path (VP) provides a connection or a set of connection between two switches. Cell networks are based on virtual circuits(VCs).All cells belonging to a single message follow the same virtual circuit and remain in their original order until they reach their destination. The First 2 VCs seems to share the same virtual path from switch I to switch III so it is reasonable to bundle these 2 VCs together to form 1VP.Similarly, other 2 VCs share the same path from switch I to switch IV, so can combine them to form 1VP.

Identifiers:

- In a virtual circuit n/w, to route data from one end point to another, the virtual connections need to be identified.
- So ATM uses a hierarchical identifier with 2 levels: a virtual path identifier (VPI)

- and a virtual circuit Identifier(VCI).
- VPI defines the specific VP and VCI defines the particular VC : inside the VP.
- VPI is the same for all virtual connections that are bundled into one VP.
- A virtual connection is defined by a pair of numbers : VPI,VCI.
- The lengths of the VPIs for UNI & NNI inter/ access are different.

Cells:

The basic data unit in an ATM / n/w is called a cell. A cell is only 53 bytes long with 5 bytes allocated to header and 48 bytes carrying payload.

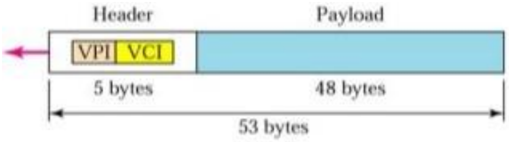


Fig 24 Cell Structure

Connection Establishment and Release:

Like x.25 and frame relay, ATM uses 2 types of connections, PVC &SVC.

PVC:

A permanent virtual circuit (PVC) connection is established between 2 end points by the network provider. The VPIs and VCIs are defined for the permanent connections & the values are entered for the tables of each switch.

SVC:

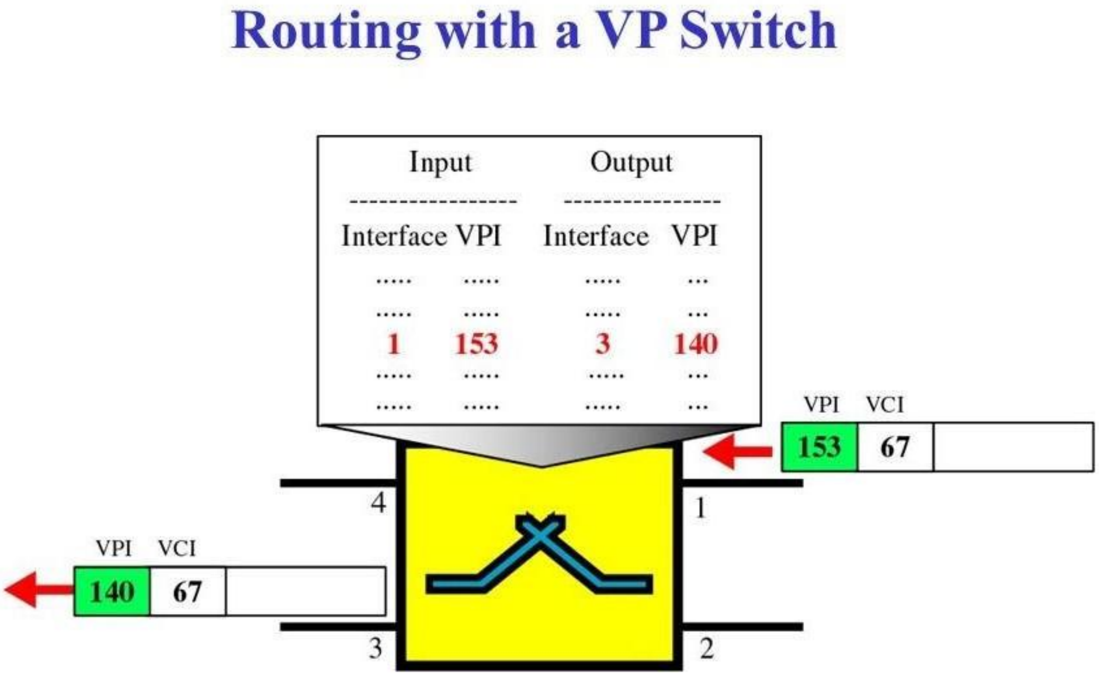
In a switched virtual circuit (SVC) connection, each time an end point wants to make a connection with another end point, a new virtual circuit should beestablished.ATM cannot do the job by itself, but needs n/w layer addresses and the services of another protocol such as B-ISDN or IP).The actual mechanism depends on the n/w layer protocol.

Switching:

ATM uses switches to route the cell from a source end point to the destination endpoint.

ATM uses 2 type of switches : VP and VPC.

VP Switch:



Routing with a VP Switch

Input		Output	
Interface	VPI	Interface	VPI
.....	.....	.....	...
.....	.....	.....	...
1	153	3	140
.....	.....	.....	...
.....	.....	.....	...

A VP switch routes the cell using only the VPI.

Fig 25 Routing with Switch

A cell with a VPI of 153 arrives at switch interface1.The switch checks its switching table, which stores four pieces of information per row: arrival interface number, incoming VPI, corresponding outgoing interface number, the new VPI.The switch finds the entry with interface 1 and VPI 153 and discovers that the combination corresponds to output interface 3 with VPI140.It changes the VPI in the header to 140and sends the cell out through interface3.

VPC switch:

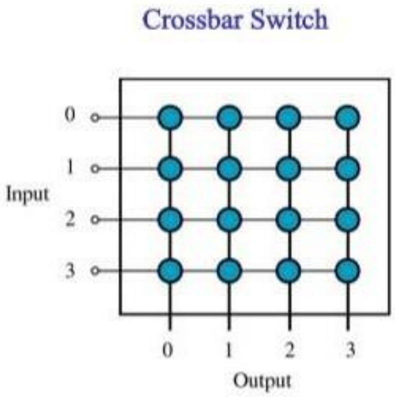
A VPC switch routes the cell using both the VPIs and the VCIs. The routing requires the whole identifier. A cell with a VPI of 153 & VCI of 67 arrives at switch interface1.The switch checks its switching table, which stores six pieces of information per row: arrival interface number, incoming VPI, incoming VCI, corresponding outing interface number, the new VPI and the new VCI. The switch finds the entry with the interface 1, VPI 153, & VCI 67 & discovers that the combination corresponds to o/p interface 3, VPI 140 &

VCI92.It changes the VPI & VCI in the header to 140 & 92, respectively, & sends the cell out through interface3.The whole idea behind dividing a virtual connection identifier into 2 parts is to allow hierarchical routing. Host of the switches in a typical ATM n/w are VP switches, they only route using VPs.The switches at the boundaries of the n/w, those that interact directly with the end point devices, use both VPIs &VCIs.

Switch Fabrics:

In ATM, there is a need for switches that can receive and route cells as fast as possible.In addition, the switches in ATM must be synchronized, although there may be no cells in some slots.The switch has a clock & delivers one cell to the output at each tick.

a. **Crossbar switch:**



- The simplest type of switch for ATM is the crossbar switch.

Fig 26 Crossbar Switch

b. **Knockout Switch:**

- The problem with the crossbar switch is the collision that result when 2 cells arriving at different inputs need to go out the same output.
- Knockout switch uses distributors & queues to direct the cells to different queues at the output.
- But still this switch is inefficient – with n i/ps& n o/ps, we still need n^2 crosspoints.

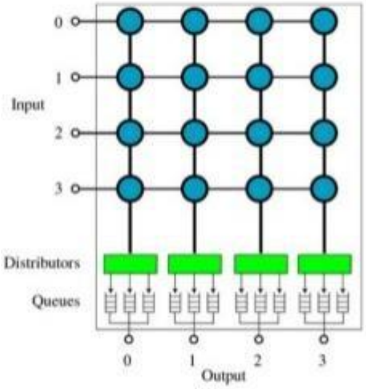


Fig 27 Knockout Switch

c. **Banyan Switch:**

- A more realistic approach is a switch called a banyan switch.
- A banyan switch is a multistage switch with micro switches at each stage that route the cells based on the o/p port represented as a binary string.
- The 1st stage routes the cell based on the high order bit of the binary string.
- The 2nd Stage routes the cells based on the second high order bit, soon.

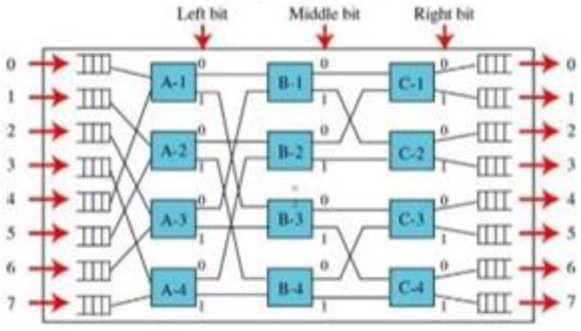
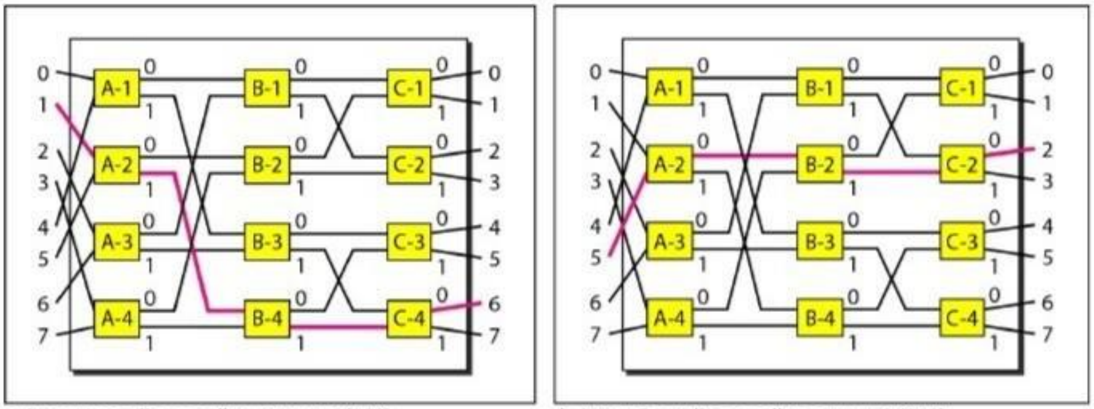


Fig 28 Banyan Switch



a. Input 1 sending a cell to output 6 (110)

b. Input 5 sending a cell to output 2 (010)

Fig 29 Operation of Banyan Switch

- The number of stages shown in figure is log2 (8) =3.
- I part(a), a cell has arrived at i/p port 1 and should go to o/p port 6 (no in binary).
- The first micro switch (A-2) routes the cell based on the 1st bit (1), the 2nd micro switch (B-4) routes the cell based on the 2nd bit (1), and the 3rd micro switch (C-4) routes the cell based on the 3rd bit(0).

d. Batcher-Banyan Switch:

- Disadvantage of banyan switch is the possibility of internal collision ever when 2 cells are not heading for the same o/p port.
- K.E. Batcher designed a switch that comes before the banyan switch & sorts the incoming cells according to their final destination. The combination is called the Batcher – banyan switch.
- Another hardware module called the trap is added between the Batcher switch and the banyan switch.

Batcher-Banyan Switch

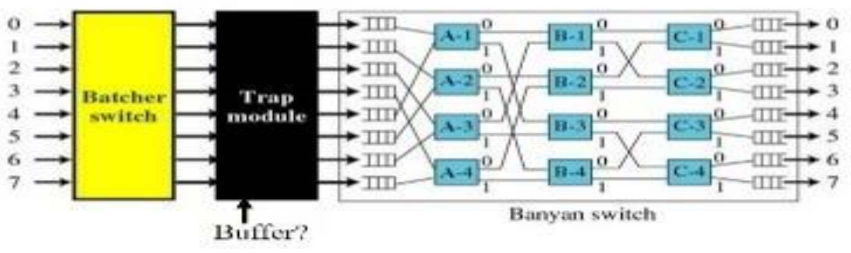


Fig 30 Batcher Banyan Switch

- The trap module prevents duplicate cells (cells with the same o/p destination) from passing to the banyan switch simultaneously.
- Only one cell for each destination is allowed at each tick, if there are more than one, they should wait for the next tick.

7. ATM Layers

ATM defines 3 layers - They are, from top to bottom, the application adaptation layer, the ATM layer, and the physical layer. The end points we all 3 layers while the switches use only the 2 bottom layers.

Application Adaptation Layer(AAL):

The AAL allows existing n/ws (such as packet n/ws) to connect to ATM facilities.AAL protocols accept transmissions from upper –layer services (eg. packet data) & map them into fixed – sized ATM cells.

These transmissions can be of any type (voice, data, audio, video) and can be of variable or fixed rates.At the receiver, this process is reversed – segments are reassembled into their original formats & passed to the receiving service.

Data Types:

- ATM designers, identified 4 types of streams i.e. data streams.

Constant-bit-rate(CBR)

CBR data refers to applications that generate & consume bits at a constant rate. In this type of application, transmission delays must be minirral& transmission must simulate real time. eg. real time voice (telephone calls) & real time video (television).

Variable bit rate(VBR):

VBR data refers to applications that generate & consume bits at variable rates.In this type of application, the bit rate varies from section to section of the transmission, but within established parameters. eg. compressed voice, data &video. Connection oriented packet data refers to conventional packet applications (such as x .25 & TCP protocol of TCP/IP) that use virtual circuits. Connectionless packet data refers to applications that use a datagram approach to routing (such as the IP protocol in TCP/IP).The ITU – T recognized the need for an additional category, one that cuts across all of the above data types but is adapted for point to point rather than multipoint or internet work transmissions.

Convergence &Segmentation:

Each of the AAL categories is actually 2 layers: the convergence sub layer (CS) and the segmentation & reassembly (SAR)sub layer.

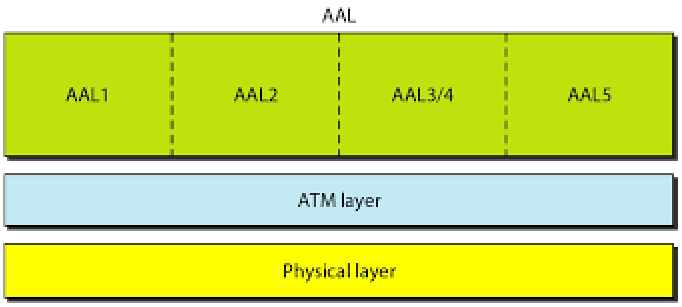


Fig 31 ATM Layers

AAL1:

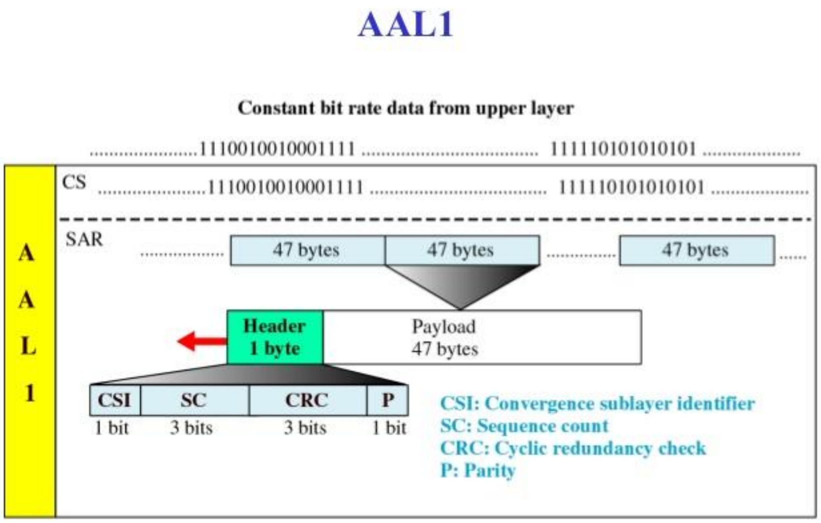


Fig 32 AAL1

Supports applications that transfer information at constant bit rates, such as video. A voice, & allows ATM to connect existing digital telephone n/ws such a DS-3 orE-1.

Convergence Sub layer(CS):

Divides the bit stream into 47 byte segments & passes them to the SAR sublayer below.

Segmentation and Reassembly(SAR):

This layer accepts a 47 byte payload from the CS & adds a one byte header.The result is a 48 byte data unit that is then passed to the ATM layer, where it is encapsulated in a cell.

The header at this layer consists of 4 fields:

Convergence sub layer identifier(CSI):

The one bit CSI field will be used for signaling purposes that are not yet clearlydefined.

Sequence Count(SC):

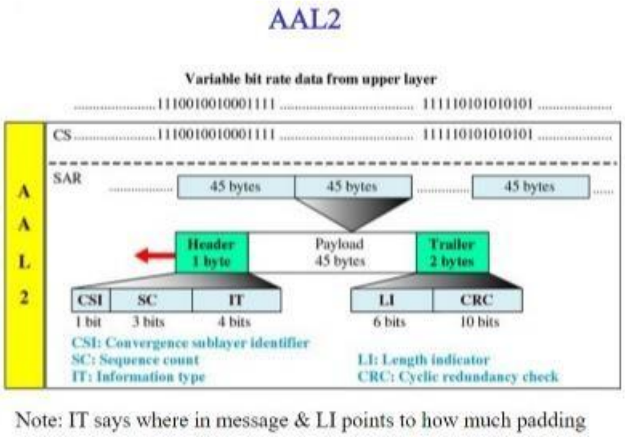
3 bit SC field is a modulo 8 sequence number to be used for ordering and identifying the cells for end to end error & flow control.

Cyclic redundancy check(CRC):

The 3 bit CRC field is calculated over the first 4 bits using the 4 bit divisor x^3+x+1.They are intended not only to detect a single or multiple bit error, but also to correct single bit errors. In non real time applications, cell can be retransmitted. In real time applications, retransmission is not an option. With no retransmission, the quality of the received data deteriorates. Large number of missing cells can destroy intelligibility. Automatic correction of single bit header errors dramatically reduces the number of cells that are missing and is ‡ a boon to quality of service.

Parity(P):

The one bit P field is a standard parity bit calculated over the first 7 bits of the header.A parity bit can detect odd number of errors but not even number of errors. If one single bit is in error, both CRC&P bit will detect it.If there are two bits in error, CRC will detect them & the P bit will not.In this case, CRC correction is invalid and the cell is discarded.



AAL2

Note: IT says where in message & LI points to how much padding

AAL2

Fig 33 AAL2

AAL2 is intended to support variable bit rate applications.

Convergence Sublayer(CS)

The format for reordering the received bit stream & adding overhead is not defined here. Different applications may use different formats.

Segmentation and Reassembly(SAR):

Functions at this layer accept a 45 byte payload from the CS and add a one byte header and two bytetrailer. The result is a 48 byte data unit that is then paned to the ATM larger, where it is encapsulated in a cell.The overhead at this layer consists of 3 fields in the header & two fields in the trailer.

Convergene Sublayer identifier (CSI):

The one bit CSI field will be used for signaling purposes that are not yet clearlydefind.

Sequence Count(SC):

The 3 bit SC field is a modulos sequence number to be used for ordering and identifying the cell for end to end error and flow control.

Information Type(IT):

The IT bits identify the data segment as falling at the beginning, middle or end of the message.

Length indicator(LI):

The first 6 bits of the trailer are used with the final segment of a message (when the IT in the header indicates the end of the message) to indicate how much of the final cell is data and how much is padding.If the original bit stream is not evenly divisible by 45, dummy bits are added to the last segment to makeup the difference. This field indicates where in the segment those bits start.

CRC:

The last 10 bits of the trailer are a CRC for the entire data unit.This can also be used to correct single bit errors in the data unit.

AAL ¾:

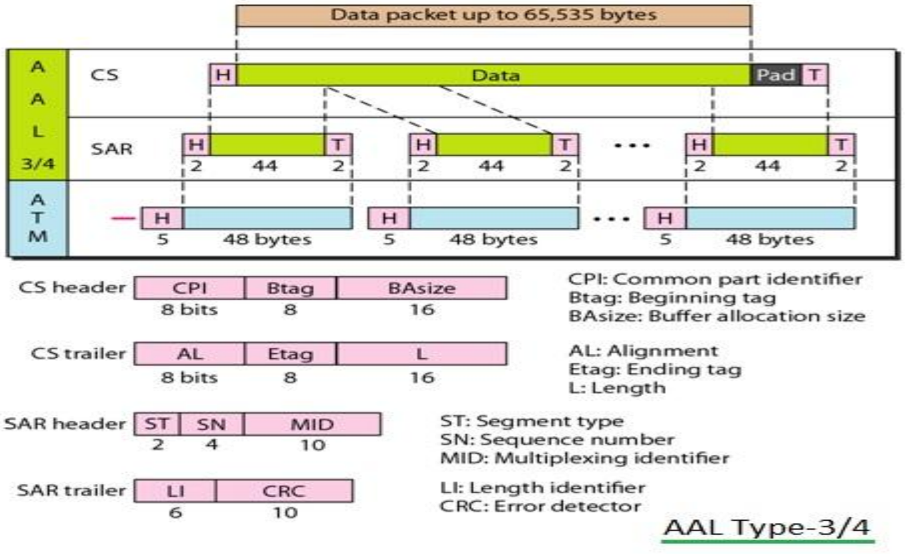


Fig 34 AAL3/4

Initially, AAL3ws intended to support connection oriented data services and AAL4 to support connectionless services. They have been combined now into a single format called AAL ¾.

Convergence Sublayer(CS):

This layer accepts a data packet of no more than 65,535 (216-1) bytes from on upper layer service and adds a header and trailer.The header and trailer indicate the beginning & end of the message, as well as how much of the final frame is data and how much ispadding. Because packets vary in length, padding may be required to ensure that segments are of the same size and that the final control fields fall where the receiver expects to find them.Once the header, trailer and padding are in place, the CS passes the message in 44 byte segments to the SAR larger.CS header and trailer are added to the beginning and end of original packet, not to every segment, the middle segments are pared to the SAR layer without addedoverhead.ATM retains the integrity of the original packets and keeps the ratio of overhead to data byte slow.the AAL ¾ CS header & trailer fields are as follows:

Type(T):

The one byte T field is a holdover from the previous version of AAL3 and is set to 0 in this format.

Begin tag(BT):

The byte BT field serves as a beginningflag.Itidentifiesthe1st cell of a segmented packet and provides synchronization for the receiving clock.

Buffer Allocation(BA):

The two byte BA field tells the receiver what size buffer is needed for the coming data.

Pad(PAD):

Padding is added when necessary to fill out the final cell(s) in a segmented packet. Total padding for a packet can be between 0 x 43 bytes and is added to the last or the last two segments.There are 3 possible padding scenarios:

- When the number of data bytes in the final segment is exactly 40, no padding is required.
- When the number of data bytes in the final segment is less than 40, we add padding bytes (40 to 1) to bring the total to40.
- When the number of data byte available for the final segment is between 41 & 44, we add padding bytes (43 to 40) to bring the total to 84. The 1st 44 bytes make a complete segment & next 40 bytes & trailer make the last segment.

Alignment(AL):

The one byte AL field is included to make the rest of the trailer four bytes long.

Ending tag(ET):

The one byte field serves as an ending flag for synchronization.

Length(L):

The two byte L field indicates the length of the data unit.

Segment and Reasembly:

Functions at this larger accept a 44 byte payload from the CS and add a 2 byte header and 1 2 byte trailer. The header and trailer at this sub layer consist of 6 fields:

Segment type(ST):

The 2 bit ST identifier cells whether the segment belongs to the beginning, middle at end of a message, or is a single – segment message.

Convergence Sub layer Identifier(CSI):

The one bit CSI field will be used for signaling purposes that are not yet clearly defined.

Sequence Count:

The 3 bit SC field is a modulo 8 sequence number to be used for ordering and identifying the cells for end to end error & flow ontrol.

Multiplexing identification(MID):

The 10 bit MID field identifies cells coming from different data flows and multiplexed on the same virtual connection.

Length indicator(LI):

The first 6 bits of the trailer are used in conjunction with ST to indicate how much of the last segment is message and how much is padding.

CRC:

The last 10 bits of the trailer are a CRC for the entire data unit.

AAL5

AAL5 assumes that all cells belonging to a single message travel sequentially and that the rest of the functions usually provided by the CS & SAR headers are already included in the upper layers of the sending application. Only padding and a 4 field trailer are added at the CS.

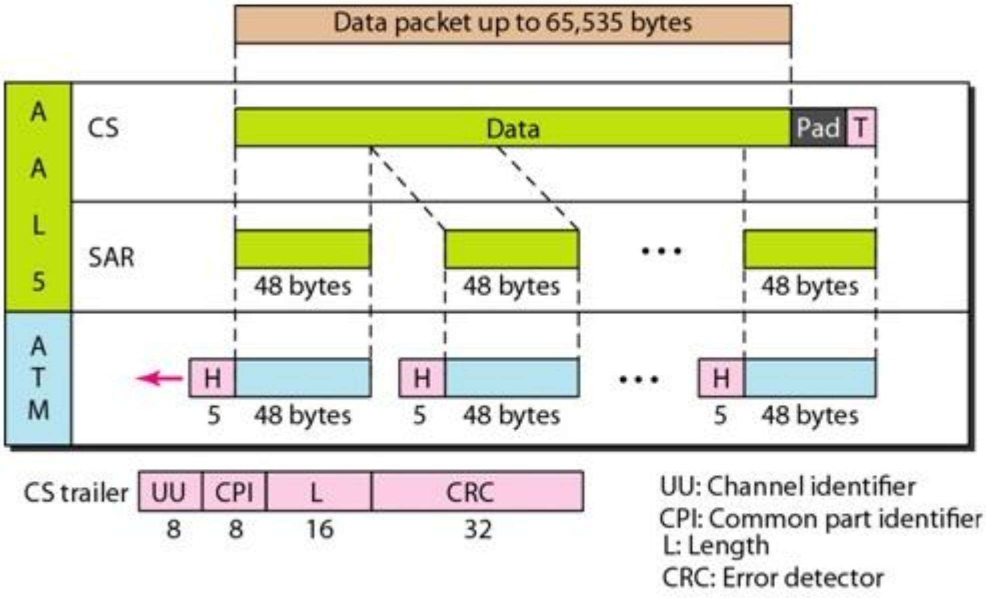


Fig 35 AAL 5

Convergence Sublayer:

This accepts a data packet of no more than 65,535 bytes from an upper layer service and adds an 8 byte trailer as well as any padding required to ensure that the position of the trailer falls where the receiving equipment expects it .Then CS panes message in 48 bytes segments to the SAR layer. Segments therefore consist of 48 bytes of data or, in the case of last segment, 40 bytes of data and of overhead(trailer). Fields added at the end of the message include the following.

Pad(PAD)

The total padding for a packet can be between 0 & 47bytes.Rules for padding same as AAL 3/4 , with the difference that body segments must equal 48 bytes rather than44.

User-to-user ID(UU):

Use of the one byte UU field is left to the discretion of the user.

Type(T):
The one byte T field is reserved but not yet defined.

Length(L):

The 2 byte L field indicates how much of the message is data & how much is padding.

CRC

The last 4 bytes are an error check for the entire data unit.

Segmentation and Reassembly:

No header or trailer is defined for the SAR level. Instead it passes the message in 48 byte segments directly to the ATM layer.

ATM layer:

The ATM layer provides routing, traffic management, switching and multiplexing services. It processes outgoing traffic by accepting 48 byte segments from the AAL sublayers and transforming them into 53 byte cells by the addition of a 5-6 byte header.

Header Format:

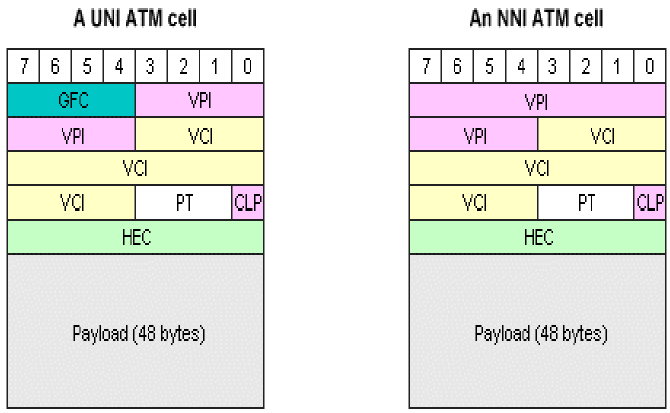


Fig 36 Header Format

ATM uses 2 formats for this header, one for user to network interface (UNI) cells & another for network to network interface (NNI)cells.

Generic flow control(GFC):

The 4 bit GFC field provides flow control at the UNI level. In the NNI header, these bits are added to the VPI. The longer VPI allows more virtual paths to be defined at the NNI level.

Virtual path identifier(VPI)

The VPI is an 8 bit field in a UNI cell and a 12 bit field in an NNIcell.

Virtual Channel Identifier(VCI):

The VCI is a 16 bit field in both frames.

Payload type(PT):

In the 3 bit PT field, the 1st bit defines the payload as user data or managerial information.

Cell loss Priority(CLP)

The one bit CLP field is provided for congestion control.When links become congested, low – priority cells may be discarded to protect the quality of service for higher priority cells.This bit indicates to a switch which cells may be dropped and which must be retained. A cell with its CLP bit set to 1 must be retained as long as there are cells with a CLP of0.

Header error correction(HEC):

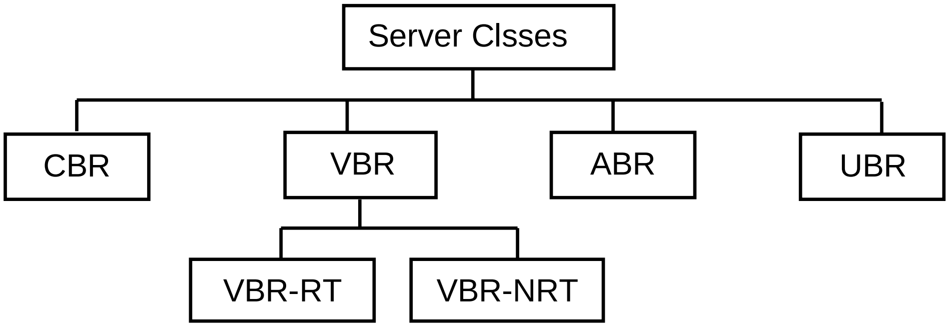
The HEC is a code computed for the first 4 bytes of the header.It is a CRC using the divisor x^8+x^2+x+1 that is used to correct single bit errors and a large class of multiple bit errors.

PhysicalLayer:

This layer defines the transmission medium, bit transmission, encoding and electrical to optical transformation. It provides convergence with physical transport protocols, such as SONET and T-3, as well as the mechanisms for transforming the flow of cells into a flow of bits.

Service Classes

The ATM Forum defines 4 service classes.



CBR:

The constant bit rate (CBR) class is designed for customers that need real time audio or video services; services is similar to T-line.

VBR:

The variable bit rate (VBR) class is divided into 2 subclasses: Real time (VBR-RT) and Non real time(VBR-NRT).VBR – RT is designed for those users that need real time services (voice, video) and use compression techniques to create a variable bit rate.

ABR:

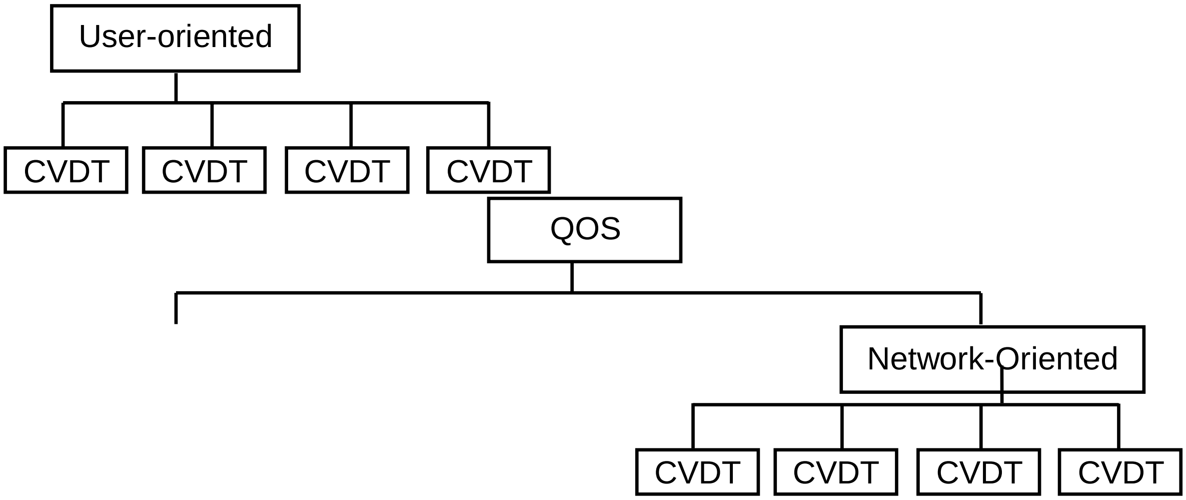
The available bit rate (ABR) class delivers cells at a minimum rate.If more network capacity is available, this minimum rate can be exceeded.

VBR:

The unspecified bit rate (UBR) class is a best effort delivery service that does not guarantee anything.

Quality of Service:

QOS defines a set of attributes related to the performance of the connection. For each connection, the user can request a particular attribute. Each service class is association with a set of the attributes.



User-Related Attributes:

These attributes define how fast the user wants to send data. The following are some user – related attributes.

SCR (Sustained Cell Rate):

SCR is the average cell rate over a long time interval.The actual cell rate may be lower or higher than this value, but the average should be equal to or less than the SCR.

PCR (Peak Cell Rate)

The PCR defines the senders maximum cell rate. The users cell rate can sometimes reach this peak, as long as the SCR is maintained.

MCR (Minimum Cell Rate)

MCR defines the minimum cell rate acceptable to the sender. eg. If MCR is 50,000, the n/w must guarantee that the sender can send atleast 50,000/- cells per second.

CVDT (Cell Variation Delay Tolerance):

CVDT is a measure of the variation in cell transmissiontimes.eg. if CVDT is 5ns, this means that the difference between the minimum and maximum delays in delivering the cells should not exceed 5 ns.

Network – Related Attributes:

These attributes are those that define characteristics of the network. The following are some network related attributes.

CLR (Cell Loss Ratio):

The CLR defines the fraction of cells lost during transmission or delivered so late that they are consideredlost.eg. IF sender sends 100 cells and one of them is last, the CLR is, CLR = 1

/ 100 = 10^{-2}

CTD (Cell Transfer Delay):

The CTD is the average time needed for a cell to travel from source to destination. The maximum CTD & the minimum CTD are also considered attributes.

CDV (Cell DelayVariation):

It is the difference between the CTD maximum and the CTD minimum.

CER (Cell Error Ratio):

It defines the fraction of the cells delivered in error.

Traffic Descriptors:

The mechanisms by which the service classes and QOs attributes are implemented are called the traffic descriptors.A traffic descriptor defines how the system enforces & polices &traffic.The algorithm to implement traffic descriptors is called the generalized cell rate algorithm (GCRA). It uses variations of leaky bucket alg. for each type of service class.

ATMWANs:

- ATM is basically a WAN technology that delivers cells over a long distance.
- Here, ATM is mainly used to connect LANs or other WANstogether. router serves as an end point between ATM n/w & othern/w.
- The router has 2 stacks of protocols : one belonging to the ATM and other belonging to the other protocol.

ATMLANs:

- The high data rate of the technology (155x622 Mbps) used in high speed LANs.
- In the figure, part a shows a switched Ethernet, part b shows an ATM LAN.
- Both use a switch to route packets or cells between computers.
- Similarity is only at surface level so a lot of issues need to be resolved. Some of them are.

Connectionless Versus Connection oriented:

- LANs such as Ethernet are connectionless protocols.
- A station sends data packets to another station whenever the packets are ready. There is no connection establishment or connection termination phase.
- ATM is a connection – oriented protocol.
- A station that needs to send cells to another station should first establish a connection and after all of the cells are sent, terminate the connection.

Physical address verses virtual connection identifiers:

A connectionless protocol (Ethernet) defines the route of a packet through source and destination addresses.A connection oriented protocol (ATM) defines the route of a cell through virtual connection identifiers (VPIs &VCIs).

Multicasting and Broadcasting delivery:

LANs such as Ethernet can both multicast and broadcast packets : a station can send packets to a group of stations or to all stations.There is no easy way to multicast or broadcast on an ATM n/w although point to multipoint connections are available.

LANE:

Local Area Network Emulation (LANE) enables an ATM switch to behave like a LAN switch : it provides connectionless service, lets the station to use their traditional address instead of VPI /VCI & allows broadcast delivery.It is based on client / server approach, all stations use LANE client (LEC) s/w & 2 servers use tow different LANE server s/w called LES &BUS.LEC s/w is installed on each station on top of the 3 ATM protocols.

The upper – layer protocols are unaware of the existence of the ATM technology.These protocols send their requests to LEC for a LAN service such as connectionless delivery using MAC unicast, multicast, or broadcast address.Th e LEC, however, just interprets the request and uses the services of either LES or BUS to do the job. The LANE server (LES) s/w is installed on the LES server.When a station receives a frame to be sent to another station using a physical address, LEC sends a special frame to the LESserver.The server creates a virtual circuit between the source and destination station.Source station uses the virtual circuit to send the frames to the destination. Multicasting and broadcasting require the use of another server called the broadcast / unknown server or BUS.

If a station needs to send a frame, the frame first goes to the BUS server, this server has permanent virtual connections to every station.Server creates copies of the received frame & sends a copy to a group of stations or to all stations, simulating a multicasting or broadcasting process.The server can also deliver a unicast frame by sending the frame to every station.In this case the destination address is unknown.This is sometimes more efficient then getting the connection identifier form the LESserver.

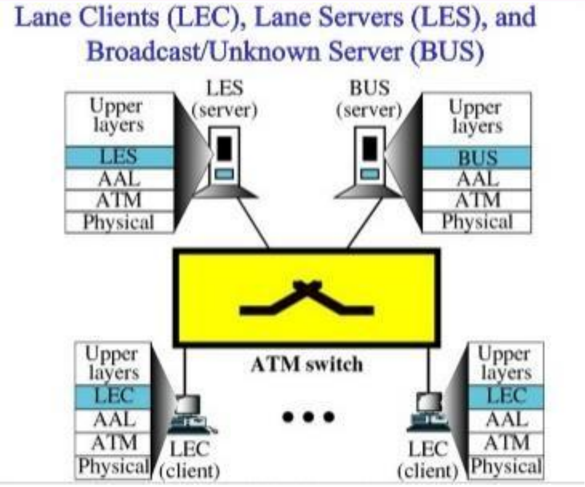


Fig 39 Local Area Network Emulation

SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

School of Computing

Department of Computer Science and Engineering

UNIT - V

Data Communication and Computer Networks-SBS1302

UNIT V - NETWORK AND APPLICATION LAYER

Repeaters Bridges Routers - Gateway - Routing algorithms - TCP/IP Network, Transport and Application Layers of TCP/IP - World Wide Web

1. Networking and Internetworking Devices

- Repeaters
- Bridges
- Routers
- Gateways
- Routing Algorithms

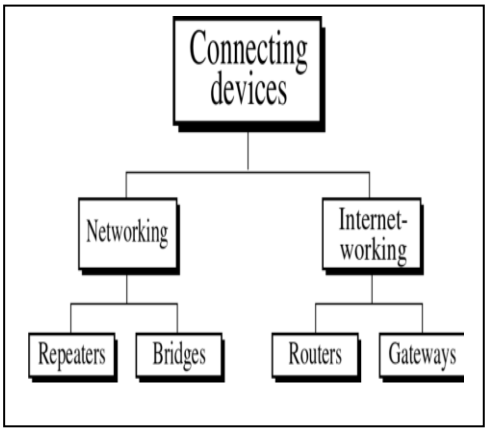
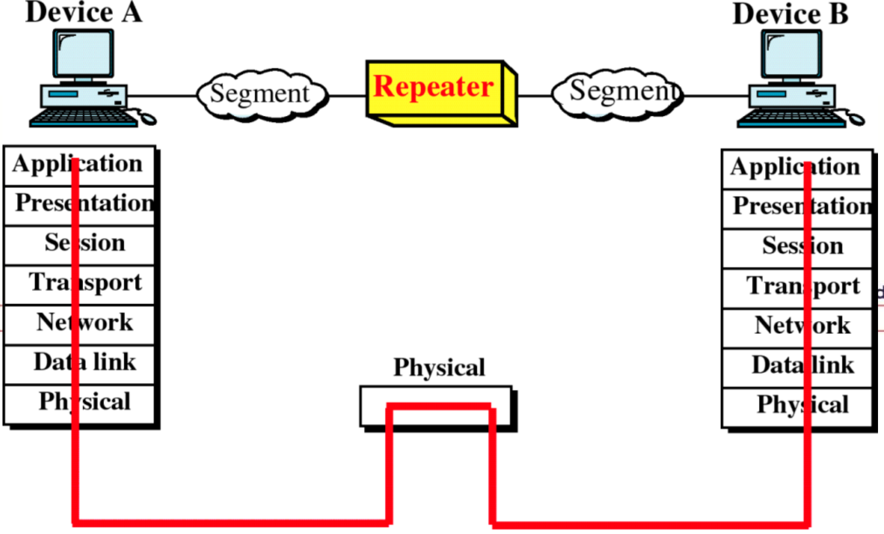


Fig 1 Connecting Devices

2. Repeaters

The repeater present in the OSImodel. Repeaters are network devices operating at physical layer of the OSI model that amplify or regenerate an incoming signal before retransmitting it. They are incorporated in networks to expand its coverage area. They are also known as signal boosters.



When an electrical signal is transmitted via a channel, it gets attenuated depending upon the nature of the channel or the technology. This poses a limitation upon the length of the LAN or coverage area of cellular networks. This problem is alleviated by installing repeaters at certain intervals.Repeaters amplifies the attenuated signal and then retransmits it. Digital repeaters can even reconstruct signals distorted by transmission loss.So, repeaters are popularly incorporated to connect between two LANs thus forming a large single LAN.

Fig 2 Operation of Repeater

As data travels through cabling systems, a certain amount of electrical interference and signal loss is inevitable. As the need for larger networks that span greater distances developed, a solution was needed to resolve signal loss over the network. Repeaters were created to regenerate and amplify weak signals, thus extending the length of the network. The basic function of a repeater is to retime, reshape, and reamplify the data signal to its original level.

- Repeaters perform no other action on the data.
- Repeaters were originally separate devices.
- Repeater may be a separate device or it may be incorporated into a hub.
- Repeaters operate at the physical layer of the OSI model

Functions of repeaters

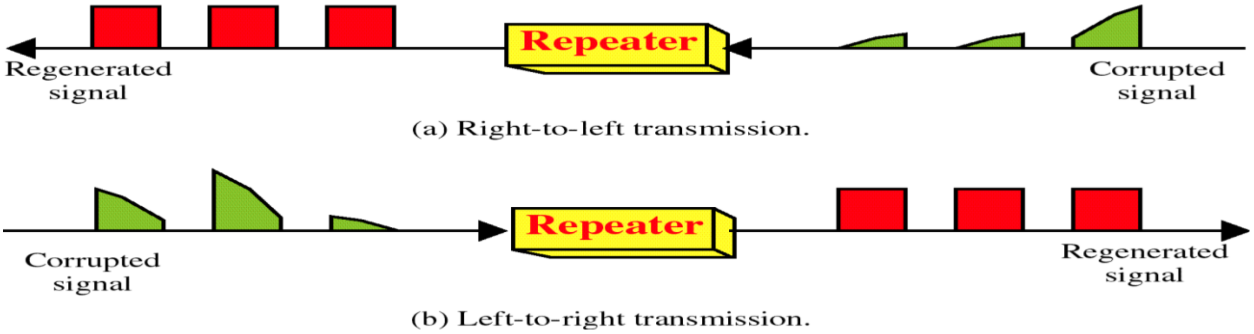


Fig 3 Functions of Repeaters

Types of Repeaters

According to the types of signals that they regenerate, repeaters can be classified into two categories −

- Analog Repeaters − They can only amplify the analog signal.
- Digital Repeaters − They can reconstruct a distorted signal.

According to the types of networks that they connect, repeaters can be categorized into two types −

- Wired Repeaters − They are used in wired LANs.
- Wireless Repeaters − They are used in wireless LANs and cellular networks.

According to the domain of LANs they connect, repeaters can be divided into two categories −

- Local Repeaters − They connect LAN segments separated by small distance.
- Remote Repeaters − They connect LANs that are far from each other.

Advantages of Repeaters

- Repeaters are simple to install and can easily extend the length or the coverage area of networks.
- They are cost effective.
- Repeaters don't require any processing overhead.
- They can connect signals using different types of cables.

Disadvantages of Repeaters

- Repeaters cannot connect dissimilar networks.
- They cannot differentiate between actual signal and noise.
- They cannot reduce network traffic or congestion.
- Most networks have limitations upon the number of repeaters that can be deployed.

3. Bridges

Bridges connect network segments typically using the same communication protocol, passing information from one network to the other. A bridge may divide an overloaded network into smaller, more efficient networks. Bridges break networks into separate segments and direct transmission to the appropriate segment much like a police officer directs automobile traffic

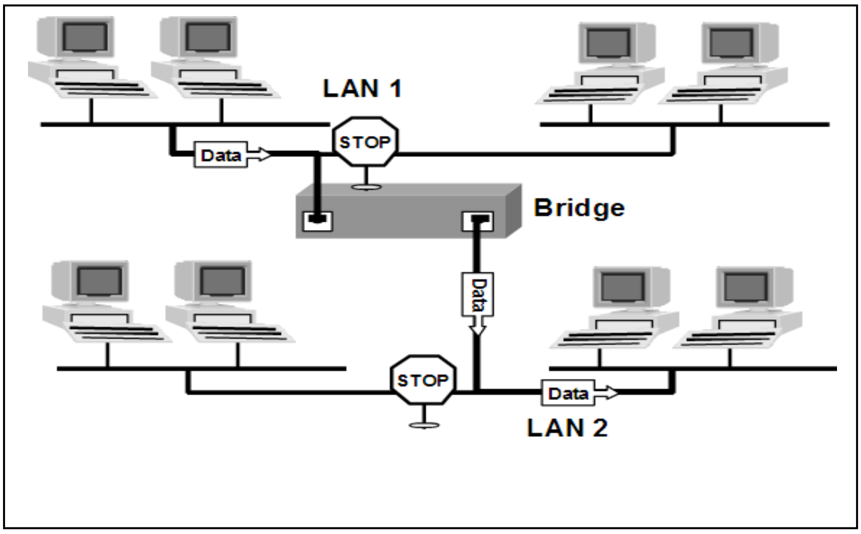


Fig 4 Operation of Bridges

ridges learn which workstations are on what network segment by looking at the hardware address in the frames it receives and entering this information into a table. Bridges function at the data link layer of the OSI model.

A bridge monitors information passing over a network segment and restricts the flow of unnecessary information. It also listens to all traffic on the segment, determines the destination address, looks up the destination address inthe table, and then passes the frame to the correct segment. Bridges can be used to connect different types of cabling from one LAN to another.

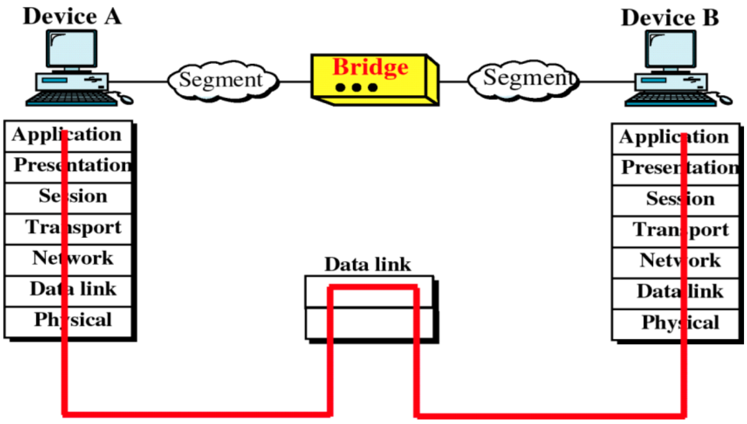


Fig 5 Functions of Bridges

Types of bridges

1. Simple bridge
2. Multiport Bridge
3. Transparent bridge

Transparent Bridge

- It is an invisible bridge in the computer network. The main function of this bridge is to block or forward the data depending on the MAC address.

- The other devices within the network are unaware of the existence of bridges. These types of bridges are most popular and operate in a transparent way to the entire networks which are connected to hosts.
- This bridge saves the addresses of MAC within a table that is similar to a routing table. This estimates the information when a packet is routed to its position.
- So it can also merge several bridges to check incoming traffic in a better way. These bridges are implemented mainly in Ethernet networks.

Translational Bridge

- A translational bridge plays a key role in changing a networking system from one type to another. These bridges are used to connect two different networks like token ring & Ethernet.
- This bridge can add or remove the data based on the traveling direction, and forward the frames of the data link layer in between LANs which uses various types of network protocols.
- The different network connections are Ethernet to FDDI/token ring otherwise Ethernet on UTP (unshielded twisted pair) to coax & in between FOC and copper wiring.

Source-route Bridge

- Source-route Bridge is one type of technique used for Token Ring networks and it is designed by IBM.
- In this bridge, the total frame route is embedded in one frame. So that it allows the bridge to make precise decisions of how the frame is forwarding using the network.
- By using this method, two similar network segments are connected to the data link layer. It can be done in a distributed way wherever end-stations join within the bridging algorithm.

Advantages

- It acts as a repeater to extend a network
- Network traffic on a segment can be reduced by subdividing it into network communications
- Collisions can be reduced.
- Some types of bridges connect the networks with the help of architectures & types of media.
- Bridges increase the available bandwidth to individual nodes because fewer network nodes share a collision domain
- It avoids waste BW (bandwidth)
- The length of the network can be increased.

- Connects different segments of network transmission

Disadvantages

- It is unable to read specific IP addresses because they are more troubled with the MAC addresses.
- They cannot help while building the network between the different architectures of networks.
- It transfers all kinds of broadcast messages, so they are incapable to stop the scope of messages.
- These are expensive as we compare with repeaters
- It doesn't handle more variable & complex data load which occurs from WAN.

Bridges connecting different LANs issues to be considered

1. Frame format
2. Payload size
3. Data rate
4. Address bit order
5. Other issues: collision, priority and acknowledgement

4. Routers

Routers link two or more different networks together, such as an Internet Protocol network. These networks can consist of various types of LAN segments, for example, Ethernet, token ring, or Fiber Distributed Data Interface (FDDI). A router receives packets and selects the optimum path to forward the packet across the network. Routers build a table of all the device addresses (routing table) across the networks. Using this table, the router forwards a transmission from the sending station to the receiving station across the best path.

Bridges know the 6-byte hardware address of all workstations on the network segment. In contrast, routers maintain a table of all learned network addresses, for example, 168.192.1.0, 168.192.2.0, and 168.192.3.0 are three IP network addresses.

Routers can increase network efficiency by filtering out broadcast traffic between networks, thus reducing unnecessary traffic between networks. Routers can connect different network types such as Ethernet, token ring, and FDDI.

Routers operate at the network level of the OSI model.

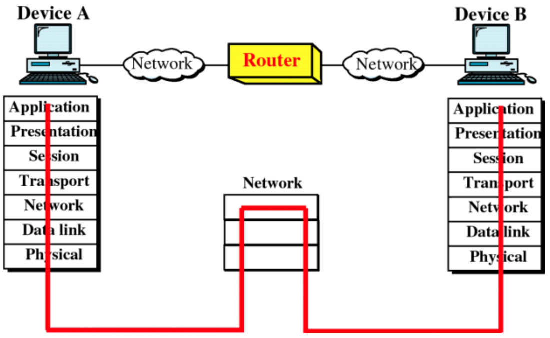


Fig 6 Functions of Routers

The routing algorithms may be classified as follows:

1. Adaptive Routing Algorithm: These algorithms change their routing decisions to reflect changes in the topology and in traffic as well. These get their routing information from adjacent routers or from all routers.
2. Non-Adaptive Routing Algorithm: These algorithms do not base their routing decisions on measurements and estimates of the current traffic and topology. Instead the route to be taken in going from one node to the other is computed in advance, off-line, and downloaded to the routers when the network is booted. This is also known as static routing.

Gateway

Gateways are multi- purpose connection devices. They are able to convert the format of data in one computing environment to a format that is usable in another computer environment (for example, AppleTalk and DECnet).

The term gateway is sometimes used when referring to a router. For the purpose of this lesson, gateways are devices that link different network types and protocols. For example, gateways translate different electronic mail protocols and convey email across theInternet.

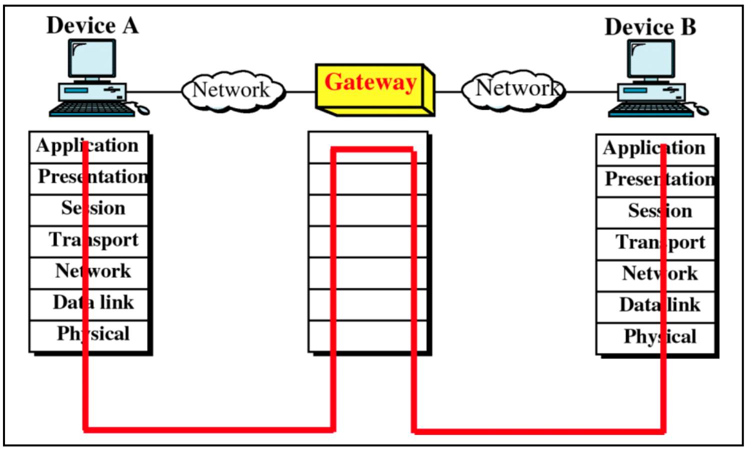


Fig 7 Functions of Gateway

Gateways can operate at all layers of the OSI model since they:

- Can provide a physical link between networks.

- Create junctions between dissimilar networks.

•Translate different network protocols and/ or applications (for example, electronic mail between the Internet and a commercial online service with its own mail protocol).

Types of Gateway:

IP gate On an Internet Protocol (IP) network:
IP packets with a destination outside a given subnet mask are sent to the network gateway. For example, if a private network has a base IPv4 address of 192.168.1.1 and has a subnet mask of 255.255.255.0, then any data addressed to an IP address outside of 192.168.1.0 is sent to the network gateway. IPv6 networks work in a

similar way. While forwarding an IP packet to another network, the gateway may perform network address translation.

Internet-to-orbit gateway:

An Internet-to-orbit gateway (I2O) connects computers or devices on the Internet to computer systems orbiting Earth, such as satellites or manned spacecraft. Project HERMES, run by the Ecuadorian Civilian Space Agency, was first to implement this kind of gateway.

Cloud storage gateway

A cloud storage gateway is a network appliance or server which translates cloud storage APIs such as SOAP or REST to block-based storage protocols such as iSCSI, Fiber Channel or file-based interfaces.

IoT gateway

An Internet of things (IoT) gateway provides the bridge between IoT devices in the field, the cloud, and user equipment such as smart phones. The IoT gateway provides a communication link between the field and the cloud, and may provide offline services and real-time control of devices in the field.

5. Routing Algorithms

Distance-Vector Routing Protocol

A **distance-vector routing (DVR)** protocol requires that a router inform its neighbors of topology changes periodically. Historically known as the old ARPANET routing algorithm (or known as Bellman-Ford algorithm).

Bellman Ford Basics – Each router maintains a Distance Vector table containing the distance between itself and ALL possible destination nodes. Distances,based on a chosen metric, are computed using information from the neighbors' distance vectors.

Information kept by DV router -

- Each router has an ID
- Associated with each link connected to a router,
- there is a link cost (static or dynamic).
- Intermediate hops

Distance Vector Table Initialization -
Distance to itself = 0
Distance to ALL other routers = infinity number

Distance Vector Algorithm –

1. A router transmits its distance vector to each of its neighbors in a routing packet.
2. Each router receives and saves the most recently received distance vector from each of its neighbors.
3. A router recalculates its distance vector when:
    - It receives a distance vector from a neighbor containing different information than before.
    - It discovers that a link to a neighbor has gone down.

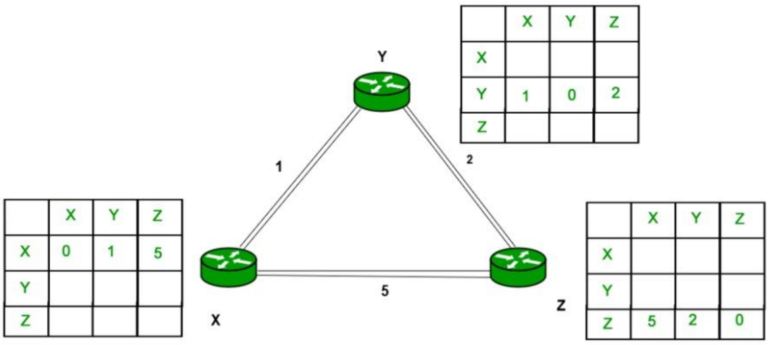
The DV calculation is based on minimizing the cost to each destination

Dx(y) = Estimate of least cost from x to y
C(x,v) = Node x knows cost to each neighbor v
Dx = [Dx(y): y ∈ N] = Node x maintains distance vector
Node x also maintains its neighbors' distance vectors
– For each neighbor v, x maintains Dv = [Dv(y): y ∈ N]

- From time-to-time, each node sends its own distance vector estimate to neighbors.
- When a node x receives new DV estimate from any neighbor v, it saves v's distance vector and it updates its own DV using B-F equation:

Dx(y) = min { C(x,v) + Dv(y), Dx(y) } for each node y ∈ N

Example – Consider 3-routers X, Y and Z as shown in figure. Each router have their routing table. Every routing table will contain distance to the destination nodes.



	X	Y	Z
X			
Y	1	0	2
Z			

	X	Y	Z
X	0	1	5
Y			
Z			

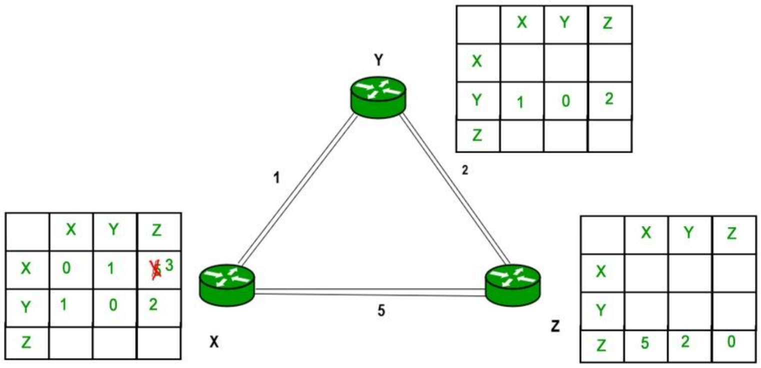
	X	Y	Z
X			
Y			
Z	5	2	0

Fig 8 Routing Table

Consider router X , X will share it routing table to neighbors and neighbors will share it routing table to it to X and distance from node X to destination will be calculated using bellmen- ford equation.

Dx(y) = min { C(x,v) + Dv(y), Dx(y) } for each node y ∈ N

As we can see that distance will be less going from X to Z when Y is intermediate node(hop) so it will be update in routing table X.



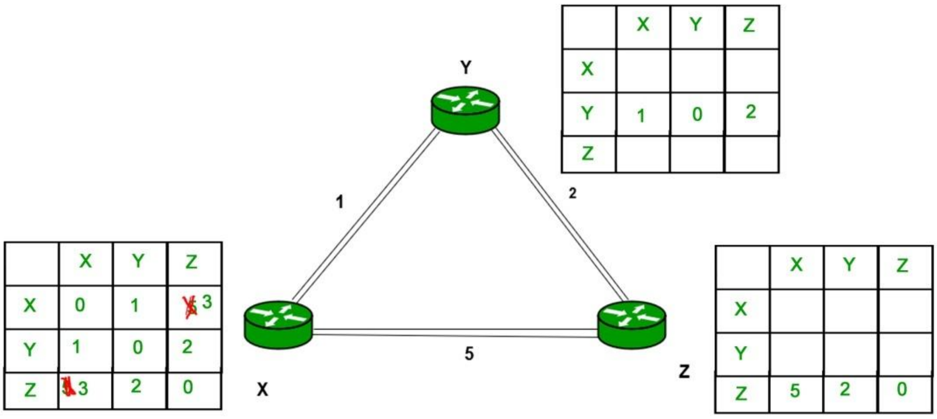
	X	Y	Z
X			
Y	1	0	2
Z			

	X	Y	Z
X	0	1	~~5~~ 3
Y	1	0	2
Z			

	X	Y	Z
X			
Y			
Z	5	2	0

Fig 9 Updated Routing Table

Similarly for Z also –



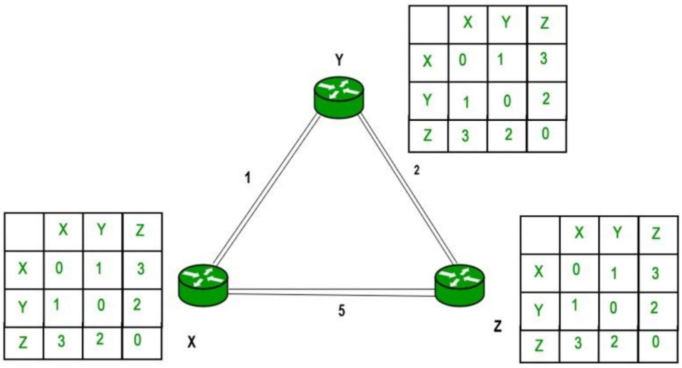
	X	Y	Z
X			
Y	1	0	2
Z			

	X	Y	Z
X	0	1	~~5~~ 3
Y	1	0	2
Z	~~5~~ 3	2	0

	X	Y	Z
X			
Y			
Z	5	2	0

Fig 10 Updated Routing table for node Z

Finally the routing table for all –



	X	Y	Z
X	0	1	3
Y	1	0	2
Z	3	2	0

	X	Y	Z
X	0	1	3
Y	1	0	2
Z	3	2	0

	X	Y	Z
X	0	1	3
Y	1	0	2
Z	3	2	0

Fig 11 Final Routing Table

Advantages of Distance Vector routing –

- It is simpler to configure and maintain than link state routing.

Disadvantages of Distance Vector routing –

- It is slower to converge than link state.
- It is at risk from the count-to-infinity problem.
- It creates more traffic than link state since a hop count change must be propagated to all routers and processed on each router. Hop count updates take place on a

periodic basis, even if there are no changes in the network topology, so bandwidth-wasting broadcasts still occur.

- For larger networks, distance vector routing results in larger routing tables than link state since each router must know about all other routers. This can also lead to congestion on WAN links.

Link State Routing

- It is a dynamic routing algorithm in which each router shares knowledge of its neighbors with every other router in the network.
- A router sends its information about its neighbors only to all the routers through flooding.
- Information sharing takes place only whenever there is a change.
- It makes use of **Dijkastra's Algorithm** for making routing tables.
- **Problems –** Heavy traffic due to flooding of packets.
  – Flooding can result in infinite looping which can be solved by using **Time to live (TTL)** field.

Link state routing is the second family of routing protocols. While distance vector routers use a distributed algorithm to compute their routing tables, link-state routing uses link-state routers to exchange messages that allow each router to learn the entire network topology. Based on this learned topology, each router is then able to compute its routing table by using a shortest path computation.

Features of link state routing protocols –

- Link state packet – A small packet that contains routing information.
- Link state database – A collection information gathered from link state packet.
- Shortest path first algorithm (Dijkstra algorithm) – A calculation performed on the database results into shortest path
- Routing table – A list of known paths and interfaces.

Calculation of shortest path –
To find shortest path, each node need to run the famous Dijkstra algorithm. This famous algorithm uses the following steps:

- **Step-1:** The node is taken and chosen as a root node of the tree, this creates the tree with a single node, and now set the total cost of each node to some value based on the information in Link State Database
- **Step-2:** Now the node selects one node, among all the nodes not in the tree like structure, which is nearest to the root, and adds this to the tree.The shape of the tree gets changed .

- **Step-3:** After this node is added to the tree, the cost of all the nodes not in the tree needs to be updated because the paths may have been changed.
- **Step-4:** The node repeats the Step 2. and Step 3. until all the nodes are added in the tree

Link State protocols in comparison to Distance Vector protocols have:

1. It requires large amount of memory.
2. Shortest path computations require many CPU circles.
3. If network use the little bandwidth ; it quickly reacts to topology changes
4. All items in the database must be sent to neighbors to form link state packets.
5. All neighbors must be trusted in the topology.
6. Authentication mechanisms can be used to avoid undesired adjacency and problems.
7. No split horizon techniques are possible in the link state routing.

Open shortest path first (OSPF) routing protocol –

- Open Shortest Path First (OSPF) is a unicast routing protocol developed by working group of the Internet Engineering Task Force (IETF).
- It is a intradomain routing protocol.
- It is an open source protocol.
- It is similar to Routing Information Protocol (RIP)
- OSPF is a classless routing protocol, which means that in its updates, it includes the subnet of each route it knows about, thus, enabling variable-length subnet masks. With variable-length subnet masks, an IP network can be broken into many subnets of various sizes. This provides network administrators with extra network-configuration flexibility. These updates are multicasts at specific addresses (224.0.0.5 and 224.0.0.6).
- OSPF is implemented as a program in the network layer using the services provided by the Internet Protocol
- IP datagram that carries the messages from OSPF sets the value of protocol field to 89
- OSPF is based on the SPF algorithm, which sometimes is referred to as the Dijkstra algorithm
- OSPF has two versions – version 1 and version 2. Version 2 is used mostly

OSPF Messages – OSPF is a very complex protocol. It uses five different types of messages. These are as follows:

- **Hello message (Type 1) –** It is used by the routers to introduce itself to the other routers.
- **Database description message (Type 2) –** It is normally send in response to the Hello message.

- **Link-state request message (Type 3) –** It is used by the routers that need information about specific Link-State packet.
- **Link-state update message (Type 4) –** It is the main OSPF message for building Link-State Database.
- **Link-state acknowledgement message (Type 5) –** It is used to create reliability in the OSPF protocol

6. TCP/IP Overview

Internet Protocol - The IP in TCP/IP

a. IP is the network layer.
b. Packet delivery service(host-to-host).
c. Translation between different data-link protocols.

TCP/IP & OSI

d. In OSI reference model terminology -the TCP/IP protocol suite covers the network and transport layers.
e. TCP/IP can be used on many data-link layers (can support many network hardware implementations).

Encapsulation

When data moves from upper layer to lower level of TCP/IP protocol stack (outgoing transmission) each layer includes a bundle of relevant information called a header along with the actual data. The data package containing the header and the data from the upper layer then becomes the data that is repackaged at the next lower level with lower layer's header. Header is the supplemental data placed at the beginning of a block of data when it is transmitted. This supplemental data is used at the receiving side to extract the data from the encapsulated data packet. This packing of data at each layer is known as data encapsulation.

7. Network Layer

Internetwork Protocol (IP)

The Internetwork Protocol (IP) is a network-layer (Layer 3) protocol that contains addressing information

and some control information that enables packets to be routed. IP has two primary responsibilities: providing connectionless, best-effort delivery of datagrams through an internetwork; and providing fragmentation and reassembly of datagrams to support data links with different maximum- transmission unit (MTU) sizes. An IP packet contains several types of information,

•Version—Indicates the version of IP currently used.

• I
P Header Length (IHL)—Indicates the datagram header length in 32-bitwords.

•Type-of-Service—Specifies how an upper-layer protocol would like a current datagram to be handled,
and assigns datagrams various levels of importance.

•Total Length—Specifies the length, in bytes, of the entire IP packet, including the data and header.

• Identification—Contains an integer that identifies the current datagram. This field is used to help piece together datagram fragments.

•Flags—Consists of a 3-bit field of which the two low-order (least-significant) bits control fragmentation. The low-order bit specifies whether the packet can be fragmented. The middle bit specifies whether the packet is the last fragment in a series of fragmented packets. The third or high-order bit is not used.

•Fragment Offset—Indicates the position of the fragment's data relative to the beginning of the data in the original datagram, which allows the destination IP process to properly reconstruct the original datagram.

•Time-to-Live—Maintains a counter that gradually decrements down to zero, at which point the datagram is discarded. This keeps packets from looping endlessly.

•Protocol—Indicates which upper-layer protocol receives incoming packets after IP processing is complete.

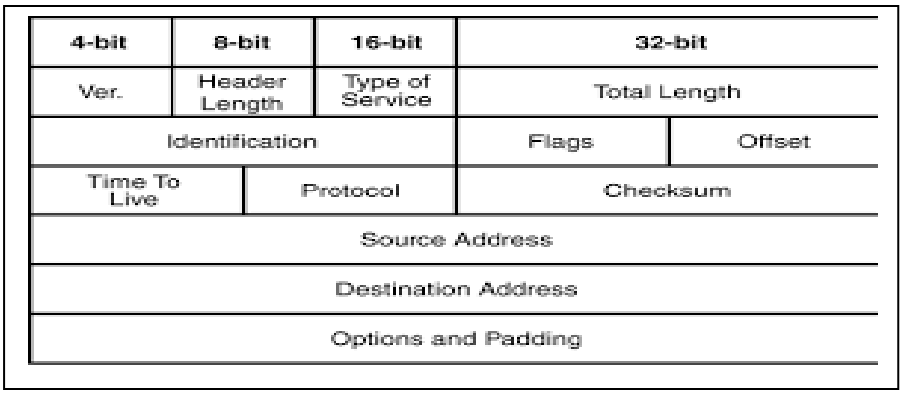
•Header Checksum—Helps ensure IP header integrity.

•Source Address—Specifies the sending node.

•Destination Address—Specifies the receiving node.

•Options—Allows IP to support various options, such as security.

•Data—Contains upper-layer information.



<table>
<tr><td>4-bit</td><td colspan="2">8-bit</td><td>16-bit</td><td colspan="2">32-bit</td></tr>
<tr><td>Ver.</td><td colspan="2">Header Length</td><td>Type of Service</td><td colspan="2">Total Length</td></tr>
<tr><td colspan="4">Identification</td><td>Flags</td><td>Offset</td></tr>
<tr><td colspan="2">Time To Live</td><td colspan="2">Protocol</td><td colspan="2">Checksum</td></tr>
<tr><td colspan="6">Source Address</td></tr>
<tr><td colspan="6">Destination Address</td></tr>
<tr><td colspan="6">Options and Padding</td></tr>
</table>

Fig 12 Packet Information

TCP/IP Addressing

The IP header has 32 bits assigned for addressing a desired device on the network. An IP address is a unique identifier used to locate a device on the IP network. To make the system scalable, the address structure is subdivided into the *network* ID and the *host* ID. The network ID identifies the network the device belongs to; the host ID identifies the device. This implies that all devices belonging to the same network have a single network ID. Based on the bit positioning assigned to the network ID and the host ID, the IP address is further subdivided into classes A, B, C, D (multicast), and E (reserved), as shown in the figure.

SUBNETTING

The concept of subnetting was introduced to overcome the shortcomings of IP addressing. Managing a large number of hosts is an enormous task. For example, a company that uses a class B addressing scheme can support up to 65,535 hosts on one network. If the company has more than one network, a multiple-network address scheme, or *subnet scheme*, is used. In this scheme, the host ID of the original IP address is subdivided into *subnet ID* and *host ID*, as shown in the figure.

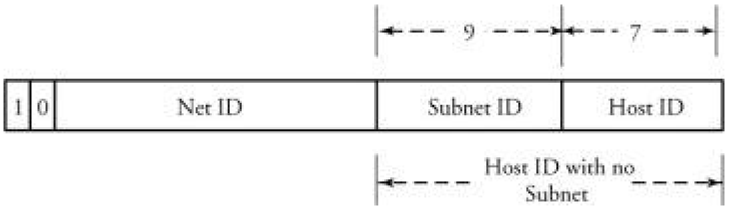


Fig 13 subnet ID and host ID

Depending on the network size, different values of subnet ID and host ID can be chosen. Doing so would prevent the outside world from being burdened by a shortage of new network addresses. To determine the sub netting number, a subnet *mask*—logic AND function—is used. The subnet mask has a field of all 0s for the host ID and a field of all 1s for the remaining field.

8. Transport Layer

Transmission Control Protocol

TCP is a connection oriented protocol and offers end-to-end packet delivery. It acts as back bone for connection. It exhibits the following key features:

a. Transmission Control Protocol (TCP) corresponds to the Transport

b. Layer of OSI Model.
c. TCP is a reliable and connection oriented protocol.
d. TCP offers:
    i. Stream Data Transfer.
    ii. Reliability.
    iii. Efficient Flow Control
    iv. Full-duplex operation.
    v. Multiplexing.
e. TCP offers connection oriented end-to-end packet delivery.
f. TCP ensures reliability by sequencing bytes with a forwarding acknowledgement number that indicates to the destination the next byte the source expect toreceive.
g. It retransmits the bytes not acknowledged with in specified timeperiod.

TCP Services

TCP offers following services to the processes at the application layer:

h. Stream Delivery Service
i. Sending and Receiving Buffers
j. Bytes and Segments
k. Full Duplex Service
l. Connection Oriented Service
m. Reliable Service

Stream Deliver Service

TCP protocol is stream oriented because it allows the sending process to send data as stream of bytes and the receiving process to obtain data as stream of bytes.

Sending and Receiving Buffers

It may not be possible for sending and receiving process to produce and obtain data at same speed, therefore, TCP needs buffers for storage at sending and receiving ends.

Bytes and Segments

The Transmission Control Protocol (TCP), at transport layer groups the bytes into a packet. This packet is called segment. Before transmission of these packets, these segments are encapsulated into an IP datagram.

Full Duplex Service

Transmitting the data in duplex mode means flow of data in both the directions at the same time.

Connection Oriented Service

TCP offers connection oriented service in the following manner:

1. TCP of process-1 informs TCP of process – 2 and gets its approval.
2. TCP of process – 1 and TCP of process – 2 and exchange data in both the two directions.

3. After completing the data exchange, when buffers on both sides are empty, the two TCP's destroy their buffers.

Reliable Service

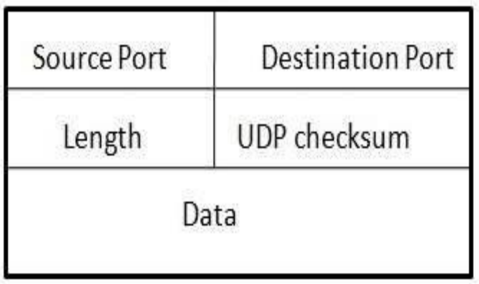
For sake of reliability, TCP uses acknowledgement mechanism.

USER DATAGRAM PROTOCOL

Like IP, UDP is connectionless and unreliable protocol. It doesn't require making a connection with the host to exchange data. Since UDP is unreliable protocol, there is no mechanism for ensuring that data sent is received.

UDP transmits the data in form of a datagram. The UDP datagram consists of five parts as shown in the following diagram:

Fig 14 UDP Datagram



Source Port	Destination Port
Length	UDP checksum
Data	

Points to remember:

n. UDP is used by the application that typically transmit small amount of data at onetime.

o. UDP provides protocol port used i.e. UDP message contains both source and destination port number, that makes it possible for UDP software at the destination to deliver the message to correct application program.

DHCP

Computers on an IP networks need some essentials information before they can communicate with other hosts. This information include an IP address, and a default route and routing prefix.

Configuring IP addressing on a large TCP/IP-based network can be a nightmare, especially if machines are moved from one network to another frequently. DHCP eliminates this manual task. The Dynamic Host Configuration Protocol (DHCP) can help with the workload of configuring systems ona network by assigning addresses to systems on boot-up automatically. It also provides a central database of devices that are connected to the network and eliminates duplicate resource assignments. DHCP server may have three methods of allocating IP-addresses:

Static allocation: The DHCP server allocates an IP address based on a table with MAC address/IP address pairs, which are manually filled only requesting clients with a MAC address listed in this table will be allocated an IP address.

Dynamic allocation: A network administrator assigns a range of IP addresses to DHCP, and each client computer on the LAN is configured to request an IP address from the DHCP server during network initialization.

Automatic allocation: The DHCP server permanently assigns a free IP address to a requesting client from the range defined by the administrator. This is like dynamic allocation, but the DHCP server keeps a table of past IP address assignments, so that it can preferentially assign to a client the same IP address that the client previously had.

Among these three method static and dynamic method are the most popular implementation.

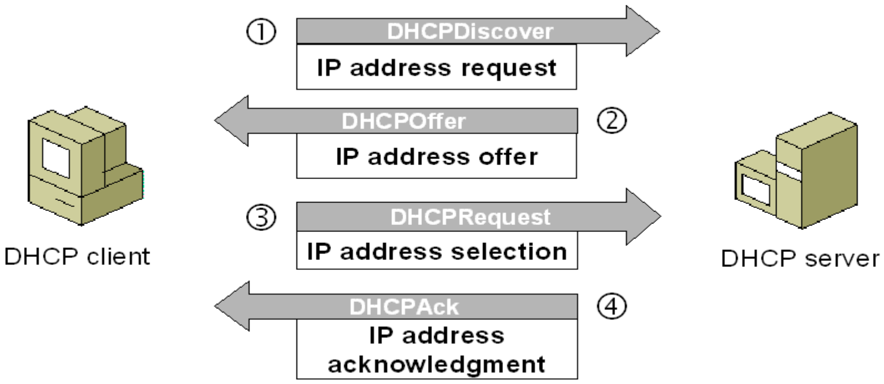


Fig 15 DHCP Protocol

TELNET

TELNET (**TEL**ecommunication **NET**work) is a network protocol used on the Internet or local area network (LAN) connections. It was developed in 1969 beginning with RFC 15 and standardized as IETF STD 8, one of the first Internet standards. Telnet was developed in 1969 to aid in remote connectivity between computers over a network.

It is a network protocol used on the Internet or local area networks to provide a bidirectional interactive communications facility. Typically, telnet provides access to a command-line interface on a remote host via a virtual terminal connection which consists of an 8-bit byte oriented data connection over the Transmission Control Protocol (TCP). User data is interspersed in-band with TELNET control information. The user's computer, which initiates the connection, is referred to as the local computer.

The computer being connected to, which accepts the connection, is referred to as the remote computer. The remote computer can be physically located in the next room, the next town or in another country.

The network terminal protocol (TELNET) allows a user to log in on any other computer on the network. We can start a remote session by specifying a computer to connect to. From that time until we finish the session, anything we type is sent to the other computer.

The Telnet program runs on the computer and connects your PC to a server on the network. We can then enter commands through the Telnet program and they will be executed as if we were entering them directly on the server console. This enables we to control the server and communicate with other servers on the network. To start a Telnet session, we must log in to a server by entering a valid username and password. Telnet is a common way to remotely control Web servers.

The term **telnet** also refers to software which implements the client part of the protocol. TELNET clients have been available on most Unix systems for many years and are available virtually for all platforms. Most network equipment and OSs with a TCP/IP stack support some kind of TELNET service server for their remote configuration including ones based on Windows NT. TELNET is a client server protocol, based on a reliable connection oriented transport. Typically this protocol used to establish a connection to TCP port 23, where a getty-equivalent program (telnetd) is listening, although TELNET predates.

Connecting to a Remote Host

Follow these steps to connect to a remote host using Telnet

1. Open Telnet by clicking on Start menu and choose run. Now type Telnet, and press Enter key from the keyboard or by clicking on the OK button.
2. From the Menu, choose Connect. Remote
3. Enter the name or IP address of the system that you want to connect to in the Host Name Field.
4. If required, a port in the Portfield.
5. In the term Type, select the type of terminal that you want Telnet to emulate.
6. After you are finished with the remote host, you can disconnect from a remote host by choosing Connect, Disconnect.

File Transfer Protocol

File Transport Protocol, or FTP, is an open protocol standard that is widely used to transport and receive large files. FTP can be used to send and receive large files. FTP can also be used to send configuration files and software updates for network switches and routers. It uses ports for communications and also uses encryption to protect the information being received and sent. In this lesson, we will go over these topics so that you can be familiar with FTP and what it has to offer.

Establishing the FTP Connection using Port 21 on the FTP Server

1. The FTP Client opens a random port on itself to initiate the request. In this case, the FTP client chooses
   Port 1.
2. The FTP Client will then forward its requests for FTP connection using its own Port 1 (this is used to
   tell the FTP server what to do i.e., 'Download', 'Stop' and 'Cancel Download') to the FTP server which
   is listening on Port 21.
3. Once the FTP server receives the FTP connection requests on its Port 21, the FTP Server willthen send
   an acknowledgment back to the FTP Client using its address of Port 1 saying that the connection is now established and download may commence.

At this point, the connection is only established between the FTP Client and the FTP Server.

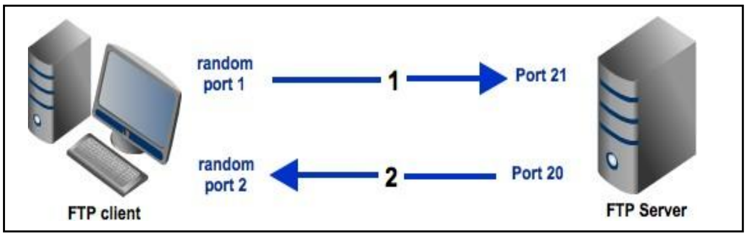


Fig 16 FTP Protocol

Establishing the FTP client to download data from Port 20 on the FTP Server

1. The FTP Client will now send a data request signal to the FTP server. In this data request, the FTP client tells the FTP server 'Hey, send me the data I want to download. Use Port 2 as my delivery address.'
2. Now that the FTP server knows to send the data to Port 2 on the FTP client, The FTP server will now open a new port which is Port 20. Port 20 is solely used to send

the data to the FTP client, nothing more. Now, using its Port 20, the FTP server will send the data to the client, using the client's Port 2 as its delivery address.

3. Once the download is complete, the client will tear down the connection if the download is successful.

Trivial File Transfer Protocol (TFTP)

Trivial File Transfer Protocol stands for Trivial File Transfer Protocol, a technology for transferring files between network devices. **TFTP** transfers the files without authentication. It is a simplified version of FTP (File Transfer Protocol).Unlike FTP, TFTP does not separate control and data information. Since there is no authentication exists, TFTP lacks in security features therefore it is not recommended to use TFTP.

Purpose of TFTP

TFTP was developed in the 1970s for computers lacking sufficient memory or disk space to provide full FTP support. Today, TFTP is also found on both consumer broadband routers and commercial network routers. Home network administrators sometimes use TFTP to upgrade their router firmware, while professional administrators may also use TFTP to distribute software across corporate networks.

How TFTP Works

Like FTP, TFTP uses client and server software to make connections between two devices. From a TFTP client, individual files can be copied (uploaded) to or downloaded from the server. TFTP uses *UDP* for transporting data.

TFTP Clients and Servers

Command line *TFTP clients* are included in current versions of Microsoft Windows, Linux and Mac OS X. Some TFTP clients with graphical interfaces are also available for free download on the Internet.

Microsoft Windows does not ship with a *TFTP server*, but several free Windows TFTP servers are available online.

Key points

- TFTP makes use of UDP for data transport. Each TFTP message is carried in separate UDP datagram.
- The first two bytes of a TFTP message specify the type of message.
- The TFTP session is initiated when a TFTP client sends a request to upload or download a file.
- The request is sent from an ephemeral UDP port to the **UDP port 69** of a TFTP server.

Address Resolution Protocol

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network.

ARP Operation

When an incoming packet destined for a host machine on a particular local area network arrives at a gateway, the gateway asks the ARP program to find a physical host or MAC address that matches the IP address. The ARP program looks in the ARP cache and, if it finds the address, provides it so that the packet can be converted to the right packet length and format and sent to the machine. If no entry is found for the IP address, ARP broadcasts a request packet in a special format to all the machines on the LAN to see if one machine knows that it has that IP address associated with it. A machine that recognizes the IP address as its own returns a reply so indicating. ARP updates the ARP cache for future reference and then sends the packet to the MAC address that replied.

Since protocol details differ for each type of local area network, there are separate ARP Requests for Comments (RFC) for Ethernet, ATM, Fiber Distributed-Data Interface, HIPPI, and other protocols.

Reverse Address Resolution Protocol

RARP is Reverse Address Resolution Protocol. This protocol resolves IP address to MAC address. To initialize the use of internet addressing on an Ethernet or other network that uses its own MAC. It allows host to communicate with other host when only the internet address of his neighbours is known. Before using IP, host sends a broad cost ARP request containing the internet address of desired destination system.

RARP (Reverse Address Resolution Protocol) is a protocol by which a physical machine in a local area network can request to learn its IP address from a gateway server's Address Resolution Protocol (ARP) table or cache. A network administrator creates a table in a local area network's gateway router that maps the physical machine (or Media Access Control - MAC address) addresses to corresponding Internet Protocol addresses. When a new machine is set up, its RARP client program requests from the RARP server on the router to be sent its IP address. Assuming that an entry has been set up in the router table, the RARP server will return the IP address to the machine which can store it for future use.

ICMP

Internet Control Message Protocol (ICMP) is a TCP/IP network layer protocol that provides troubleshooting, control and error message services. ICMP is most frequently used in operating systems for networked computers, where it transmits error messages. ICMP for Internet Protocol version 4 is called ICMPv4 and for Internet Protocol version 6 is called ICMPv6. Internet Control Message Protocol is also known as RFC 792.

An ICMP message is created as a result of errors in an IP datagram or for diagnostic routing purposes. These errors are reported to the originating datagram's source IP address. An ICMP message is encapsulated directly within a single IP datagram and reports errors in the processing of datagrams.

An ICMP header begins after the IPv4 header. An ICMP packet has an eight-byte header, followed by a variable-sized data section. The first four bytes of the header are fixed:

- ICMP type
- ICMP code
- Checksum of the entire ICMP message
- Checksum of the entire ICMP message

The remaining four bytes of the header vary based on the ICMP type and code.

The error message associated with ICMP includes a data section that holds the entire IP header along with the first eight bytes of the packet that generated the error message. An ICMP datagram is then encapsulated in a new datagram.

IGMP

Internet Group Management Protocol (IGMP) is a communications protocol that enables a node (receiver) to inform a multicast router (IGMP querier) of the node’s intention to receive particular multicast traffic.

IGMP runs between a router and a node that enables the following actions:

- Routers ask nodes if they need a particular multicast stream (IGMPquery).
- Nodes respond to the router if they are seeking a particular multicast stream (IGMP reports). The IGMP communication protocol is used by the nodes and the adjacent routers on IP networks to interact and to establish ground rules for multicast communication and establish multicast group membership.

IGMP snooping

IGMP snooping is an activity performed by switches to track the IGMP communications related packet exchanges and adapt to filtering the multicast packets. Switches featuring IGMP snooping derive useful information by observing these IGMP transactions between the nodes and routers. This function enables the switches to correctly forward the multicast packets, when needed, to the next switch in the network path.

Switches monitor the IGMP traffic and only send out multicast packets when necessary. A switch typically builds an IGMP snooping table that has a list of all the ports that have requested a particular multicast group. The IGMP snooping table is used to allow multicast packets to travel across the network or to disallow them from traveling across the network. You can configure your switch to avoid IGMP snooping.

SNMP

SNMP (Simple Network Management Protocol) is the protocol that can be used for monitoring and managing hosts in network. Network may be LAN or WAN whatever. Hosts may be routers, switches, servers, workstations, printers, modem and more. Every host under network will be monitoring and managing by SNMP. SNMP have 3 main parts. Those are

- Managed device
- Agent - Software which runs on managed devices
- Network management system (NMS) — Software which runs on the manager

Managed Device

The managed device is normally a host in network (or network elements). As above it may be router, switch, client computer, server etc. It implements an SNMP interface that allows unidirectional (read-only) or bidirectional (read and write) access to node-specific information. Managed devices exchange node-specific information with theNMSs.

Agent:

Agent is a software running in Managed device. This software acts as an agent. That means, software will get the information about managed device and send it to NMS. The information is related with software, hardware installed in managed device, network traffic and related information. We can tell that information as log. Depend upon the agent, our work maybe monitoring or managing. If we have read access to the managed device via agent, we can do the monitoring alone. If we have write access to the managed device we can do the managing operation.

NMS:

NMS (Network Management System) is combination of manager system (mostly server) and software of managing. (It's not like agent). It executes applications that monitor and control managed devices. NMSs require bulk amount of the processing and memory resources. One or more NMSs may exist on any managed network.

Management Information base (MIB)

MIB is a virtual database used for managing the entities in a communications network. Most often associated with the Simple Network Management Protocol (SNMP), the term is also used more generically in contexts such as in OSI/ISO Network management model. While intended to refer to the complete collection of management information available on an entity, it is often used to refer to a particular subset, more correctly referred to as MIB-module. MIBs use the notation defined by ASN.1 Note: **Abstract Syntax Notation One** (**ASN.1**) is a standard and flexible notation that describes data structures for representing, encoding, transmitting, and decoding data. It provides a set of formal rules for describing the structure of objects that are independent of machine-specific encoding techniques and is a precise, formal notation that removes ambiguities.

Protocol details

SNMP operates in the Application Layer of the Internet Protocol Suite (Layer 7 of the OSI model).

The SNMP agent receives requests on UDP port 161. The manager may send requests from any available source port to port 161 in the agent. The agent response will be sent back to the source port on the manager. The manager receives notifications (*Traps* and *Inform Requests*) on port 162. The agent may generate notifications from any available port.

The seven SNMP protocol data units (PDUs) are as follows:

Get Request

A manager-to-agent request to retrieve the value of a variable or list of variables. Desired variables are specified in variable bindings (values are not used). Retrieval of the specified variable values is to be done as an atomic operation by the agent. A *Response* with current values is returned.

SetRequest

A manager-to-agent request to change the value of a variable or list of variables. Variable bindings are specified in the body of the request. Changes to all specified variables are to be made as an atomic operation by the agent. A Response with (current) new values for the variables is returned.

Get Next Request

A manager-to-agent request to discover available variables and their values. Returns a Response with variable binding for the lexicographically next variable in the MIB. The entire MIB of an agent can be

walked by iterative application of Get Next Request starting at OID 0. Rows of a table can be read by specifying column OIDs in the variable bindings of the request.

Get Bulk Request

Optimized version of Get Next Request. A manager-to-agent request for multiple iterations of Get Next Request. Returns a Response with multiple variable bindings walked from the variable binding or bindings in the request. PDU specific non-repeaters and max-repetitions fields are used to control response behavior. Get Bulk Request was introduced in SNMPv2.

Response

Returns variable bindings and acknowledgement from agent to manager for Get Request, Set Request, Get Next Request, Get Bulk Request and Inform Request. Error reporting is provided by error-status and error-index fields. Although it was used as a response to both gets and sets, this PDU was called Get Response in SNMPv1.

Trap

Asynchronous notification from agent to manager. Includes current sysUpTime value, an OID identifying the type of trap and optional variable bindings. Destination addressing for traps is determined in an application-specific manner typically through trap configuration variables in the MIB. The format of the trap message was changed in SNMPv2 and the PDU was renamed SNMPv2- Trap.

Inform Request

Acknowledged asynchronous notification from manager to manager. This PDU uses the same format as the SNMPv2 version of Trap. Manager-to-manager notifications were already possible in SNMPv1 (using a Trap), but as SNMP commonly runs over UDP where delivery is not assured and dropped packets are not reported, delivery of a Trap was not guaranteed. Inform Request fixes this by sending back an acknowledgement on receipt. Receiver replies with Response parroting all information in the Inform Request. This PDU was introduced in SNMPv2.

9. World Wide Web

The Internet and the World Wide Web

The Internet is a collection of computers, all connected to one another. It first got its start in 1966 as the *ARPANET*, a project of the Defense Department's **A**dvanced **R**esearch **P**rojects **A**gency. At some point it was opened up to university researchers, and, for many years, was used primarily for transferring email and files among university researchers and for exchanging information via *newsgroups*. Each computer that is connected to the network is called an *internet host*. In 1986 there were 5,000 hosts and 241 newsgroups.

In 1990, Tim Berners-Lee came up with the idea of having a large number of documents, all of which could be linked together and refer to one another. He called this set of documents the World Wide Web (WWW). Each person or organization's collection of documents was called a website. The idea caught on quickly. In 1993 there were 600 websites. (The Internet itself was still growing; there were now two million Internet hosts.) In 1995 there were 100,000 websites. Today there are literally millions of websites, and the number of Internet hosts has grown as well.

Clients and Servers

Each Internet host can act as a server, or a repository files. Some hosts hold email files, some hold newsgroup postings, and others hold web pages. A server's purpose in life is to wait for requests to come in from some client, find the requested file or page, and send it back to the client. A client is usually an end user's computer.

Think of it as a store. You're the client; you go in and ask the server for a particular item. He goes back to where all the products are stored, prepares the item, and brings it out to you.

Similarly, when you sit at your computer, you request a particular file. That request goes to the appropriate server, which finds the file and sends it back to you. The software that you use depends on the kind of files you want. If you are requesting web pages, you use a browser. If you are requesting email, you use a program designed for reading mail. If you're reading newsgroup posts, you may use a special news reader program. For your convenience, the latest browsers have combined all these functions into various sections of a single program.

In the first assignment for this course, you will set up an account for yourself on a Windows machine, which will be the machine that you use as a client. You will also set up an account on a UNIX machine which will serve files to you.

HTML

Before the WWW, people exchanged just plain text files or they exchanged files in some proprietary format. One of Berners-Lee's objectives was to create a way to write files that would improve upon plain text, but be open to everyone. That method is HTML, which stands for **H**yper **T**ext **M**arkup **L**anguage.

Markup

Markup comes from the bad old days before word processors. If you needed a brochure, you'd type it on a typewriter, and then literally mark it up with a red pen to tell the typesetter what you wanted it to look like. The typesetter would follow your instructions and return a finished document to you.

Hypertext

In addition to elements that let you specify how a document should be structured and presented, HTML has tags that let you tell how your document should be linked to other documents on the WWW. This ability to link documents together is called *hypertext*. The term was invented in 1965 by Ted Nelson, but the idea itself has been around since 1945.

HTML, XHTML, and HTML5

The rules for how you write proper HTML (before version 5) are defined by the Standard Generalized Markup Language (*SGML*) rulebook. In recent years, a new rulebook known as *XML*, the Extensible Markup Language has emerged. It is not as powerful as the SGML rulebook, but it is far simpler. When we write HyperText Markup Language according to the rules of SGML, we call it HTML. When we write the same elements according to the rules of XML, we call it XHTML. The newest version, HTML5, lets you write your markup in either HTML or XHTML syntax.

HTML Documents

HTML documents consist of text with tags. Tags are commands written between less than (<) and greater than (>) signs, also known as *angle brackets*. Here's an example of the tag that tells the browser to use boldface text:

This is a <b>special message</b> for you!

The opening tag, closing tag, and the content in between are collectively called an *HTML element*. Technically, tags and elements are very different, but most people use the terms interchangeably.

Things to remember about tags:

- Don't leave a space after the opening <sign.
- The closing tag has the same command name as the opening tag, and it has a forward slash (/) after the<.
- When using XHTML syntax, every opening tag *must* have a closing tag.
- In XHTML syntax, the tag names and attribute names *must* be written entirely in lowercase. XHTML is known as a *case-sensitive* markup language.

The Document Template

Build a *template* HTML5 file; a "framework" that can be copied and filled in. All our HTML5 files will be built on this framework.

Open a new file, and type the opening and closing <html> tag. This tag is a *structure* tag; it tells the browser that the entire document will be between these tags. Leave some blank lines between the opening and closing tags; you'll be putting things in between themlater.

```
<html>
</html>
```

Now add this to the opening tag; it lets the browser know that the primary language of this document isEnglish:

```
<html xml:lang="en" lang="en">
</html>
```

Business letters have a head and a body. The head gives identifying information (who it's from, whom it's to, the date, etc.). The body contains the actual content of the letter. Similarly, our HTML documents will also have a head and a body. Add the opening and closing <head> and <body> tags to yourtemplate:

```
<html xml:lang="en"lang="en">
<head>
</head>
```

```
<body>
</body>
</html>
```

Put a title in the head of the document. This is identifying information. Some search engines use it to index your files. If you bookmark a page, the title of the document is used as the bookmark text. Add a <title>tag:

```
<html xml:lang="en"lang="en">
<head>
<title>Put a TitleHere</title>
</head>
<body>
</body>
</html>
```

Since it is the *world wide web*, not all web pages are in English. You can specify, for example, that a page is written entirely with Russian or Chinese characters. In our case, we'll add the <meta> element to specify that we are using a "universal" character set called Unicode.

```
<html xml:lang="en" lang="en">
<head>
  <title>Put a Title Here</title>
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
</head>

<body>

</body>
</html>
```

Note: there is a simpler way to specify the character set, but it does not work on all browsers. The
<meta> element given here works on all modern browsers.

In order to get the best of all possible worlds—a document that can be processed either as XHTML or HTML5, you must add a *namespace declaration*; it lets XML processing tools know which elements are part of HTML. This is useful when you have a document that contains markup from several different markup languages.

```
<html xml:lang="en" lang="en" xmlns="http://www.w3.org/1999/xhtml">
<head>
  <title>Put a Title Here</title>
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
</head>

<body>

</body>
</html>
```

The template is almost finished. Two things must be added at the beginning of the document. The first thing is a *Document Type Declaration*. The Document Type Declaration (DTD) **must** be the very first line in your document; do not leave a blank line before it. The DTD is *not* a tag! It is a declaration, which declares to the browser precisely which "flavor" of HTML the document uses. The very latest browsers will use the declaration to determine how certain tags should be displayed. When using HTML5, the document type declaration is very simple.

```
<!DOCTYPE html>

<html xml:lang="en" lang="en" xmlns="http://www.w3.org/1999/xhtml">
```

```
<head>
   <title>Put a Title Here</title>
   <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
</head>

<body>

</body>
</html>
```

Finally, add an *HTML comment* to tell who wrote the file. You put comments in a document for the benefit of other humans who will be reading it. The browser ignores it completely and they can be more than one line long) go between the opening <!-- and the closing -->. This is a comment, it’s not a tag, so it has its own rules.

```
<!DOCTYPE html>

<!-- Written by E.G. Valley, 4 Sep 2010 -->

<html xml:lang="en" lang="en" xmlns="http://www.w3.org/1999/xhtml">
<head>
   <title>Put a Title Here</title>
   <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
</head>
<body>
</body>
</html>
```