SPPU New Syllabus

A Book Of

COMPUTER NETWORKS

For B.C.A.(Science) : Semester - III

[Course Code 233 : Credit - 4]

CBCS Pattern

As Per New Syllabus, Effective from June 2020

Dr. Ms. Manisha Bharambe
M.Sc(Comp. Sci),M.Phil, Ph.D(Comp. Sci)
Vice Principal and Associate Professor,
Computer Science Department,
MES Abasaheb Garware College,
Pune 4

Mrs. Veena Gandhi
M.C.S., M.Phil (Comp. Sci.), UGC-NET
Assistant Professor,
Computer Science Department,
Abeda Inamdar Senior College,
Pune 1

Rahul Patil
M.C.S.
Lecturer and Head of Computer Science Dept.,
N.D.M.V.P. Samaj's K.T.H.M. College,
Nasik

Price ₹ 260.00

NIRALI PRAKASHAN
ADVANCEMENT OF KNOWLEDGE

N5413

Syllabus ...

Unit I: Introduction to Data Communications Computer Networks **8 Hrs**

1.1 Data communications, Characteristics of Data Communication

1.2 Components of Data communication

1.3 Data Representation – Text, Numbers, Images, Audio, Video

1.4 Types of Data flow – Simplex, Half Duplex, Full Duplex

1.5 Computer Networks applications – Business Application, Home Application, Mobile User

1.6 Broadcast and point-to-point networks

1.7 Network Topologies - Bus, Star, Ring, Mesh

1.8 Network Types - LAN, MAN, WAN, PAN, Wireless Networks, Home Networks, internetworks

1.9 Protocols and standards – Definition of a Protocol, Protocol standards: De facto and De jure

Unit II: Network Models **8 Hrs**

2.1 OSI Model – layered architecture, peer-to-peer processes, encapsulation

2.2 TCP/IP Model – layers and Protocol Suite

2.3 Addressing-Physical, Logical, Port addresses, Specific addresses

Unit III: Physical Layer **10 Hrs**

3.1 Analog and Digital data, Analog and Digital signals, Digital Signals-Bit rate, Bit length

3.2 Baseband Transmission, Broadband Transmission

3.3 Transmission Impairments– Attenuation, Distortion and Noise

3.4 Data Rate Limits– Noiseless channel: Nyquist's bit rate, noisy channel : Shannon's law

3.4 Performance of the Network Bandwidth, Throughput, Latency (Delay), Bandwidth – Delay Product, Jitters

3.4 Line Coding Characteristics, Line Coding Schemes–Unipolar -NRZ, Polar-NRZ-I, NRZ-L, RZ, Manchester and Differential Manchester, Problems

3.5 Transmission Modes, Parallel Transmission and Serial Transmission– Asynchronous and Synchronous and Isochronous

3.6 Multiplexing FDM and TDM

3.7 Switching-Circuit Switching, Message Switching and Packet Switching.

3.6 Multiplexing FDM and TDM

3.7 Switching-Circuit Switching, Message Switching and Packet Switching

Unit IV: Data Link Layer **10 Hrs**

4.1 Framing – Concept, Methods – Character Count, Flag bytes with Byte Stuffing, Starting & ending Flags with Bit Stuffing

4.2 Error detection code – Hamming Distance, CRC

4.3 Elementary data link protocols – Simplex stop & wait protocol, Simplex protocol for noisy channel, PPP, HDLC

4.4 Sliding Window Protocols – 1-bit sliding window protocols, Pipelining – Go-Back N and Selective Repeat

4.5 Random Access Protocols – ALOHA – pure and slotted, CSMA-1- persistent, p-persistent and non-persistent CSMA/CD,CSMA/CA

4.6 Controlled Access – Reservation, Polling and Token Passing

4.7 Channelization – Definitions – FDMA, TDMA and CDMA

Unit V: Network Layer **10 Hrs**

5.1 IPv4 addresses: Address space, Notation, Classful addressing, Classless addressing, NAT, Sub netting, Super netting

5.2 IPv4: Datagram, Fragmentation, checksum, options

5.3 IPv6 addresses: Structure, address space

5.4 IPv6: packet format, Extension headers

Unit VI: Transport and Application Layer **12 Hrs**

6.1 Process-to-Process Delivery, Multiplexing and De-multiplexing

6.2 User Datagram Protocol (UDP) - Datagram Format, Checksum, UDP operations, Use of UDP

6.3. Transmission Control Protocol (TCP) - TCP Services – Process to-Process Communication, Stream Delivery Service, Sending and Receiving Buffers, Segments, Full – Duplex Communication, Connection oriented service, Reliable service

6.4 TCP Features – Numbering System, Byte Number, Sequence Number, Acknowledgement Number, Flow Control, Error Control, Congestion Control

6.5 TCP Segment Format

6.6 TCP Vs UDP

6.6 Domain Name System (DNS) - Distribution of Name Space, DNS in the Internet

6.7 E-MAIL - Architecture, User Agent, Message Transfer Agent - SMTP, Web Based Mail

6.8 WWW - Architecture

6.9 HTTP - HTTP Transaction

❖❖❖

Contents ...

1.	**Introduction to Data Communications and Computer Networks**	**1.1 – 1.42**
2.	**Network Models**	**2.1 – 2.26**
3.	**Physical Layer**	**3.1 – 3.46**
4.	**Data Link Layer**	**4.1 – 4.62**
5.	**Network Layer**	**5.1 – 5.36**
6.	**Transport and Application Layer**	**6.1 – 6.38**

❖❖❖

1...

Introduction to Data Communications & Computer Networks

Objectives...

- To understand Concepts of Computer Network and Data Communication.
- To learn Applications of Computer Network.
- To learn Types of Data Flows.
- To study Network Topologies and Types.
- To study Types of Networks.

1.1 INTRODUCTION

- When we communicate, we share information. This sharing can be local or remote. Local communication can be face to face between individuals, while remote communication takes over distance. To transfer, share the information remotely or locally we need to interconnect the computers.
- Communication is the basic process of information exchange. In electronic communication, information or messages in the form of electrical signals are propagated from one point to another by electronic means.
- Data communication refers to the exchange of data/information between two devices through some form of wired transmission medium (like coaxial cable, optic fiber cable etc.) or wireless transmission medium (like radio waves, micro waves, satellite communication and so on).
- Networking is linking of more than two different entities together to form a group or network to perform some specific task.
- The networking enhances the capacity of computer to share, exchange, preserve and protect information.

- In this chapter we are going to study all fundamental things about data communication, computer network, how networks operate, types of networks, and types of topologies available, etc.

1.2 DATA COMMUNICATION

- Communication, between human beings or computer systems, involves transfer of information from a sender to a receiver.
- Data Communication is the exchange of data/information between two devices using some transmission media such as cable wire or optic fiber.

1.2.1 Characteristics of Data Communication (S-18, 19)

- The effectiveness of data communication depends on the following four factors/characteristics:
  1. **Delivery:** The data must reach to the correct destination (user or device).
  2. **Accuracy:** The data delivered by the system should be accurate.
  3. **Timeliness:** The data delivered by the system must be in timely manner. If it is delayed then data becomes useless. In real time system, the data such as audio or video should be deliver in the same order as they are produced.
  4. **Jitter:** Jitter means variation in the packet arrival time. It is uneven delay of audio or video packets. For example, if sender sends each packet after 20 ms, but at receiver some packets arrives at 20 ms and some are after 30 ms. So jitter is 10 ms for the delayed packets.

1.2.2 Components of Data Communication

- The Fig 1.1 shows the five components of data communication.

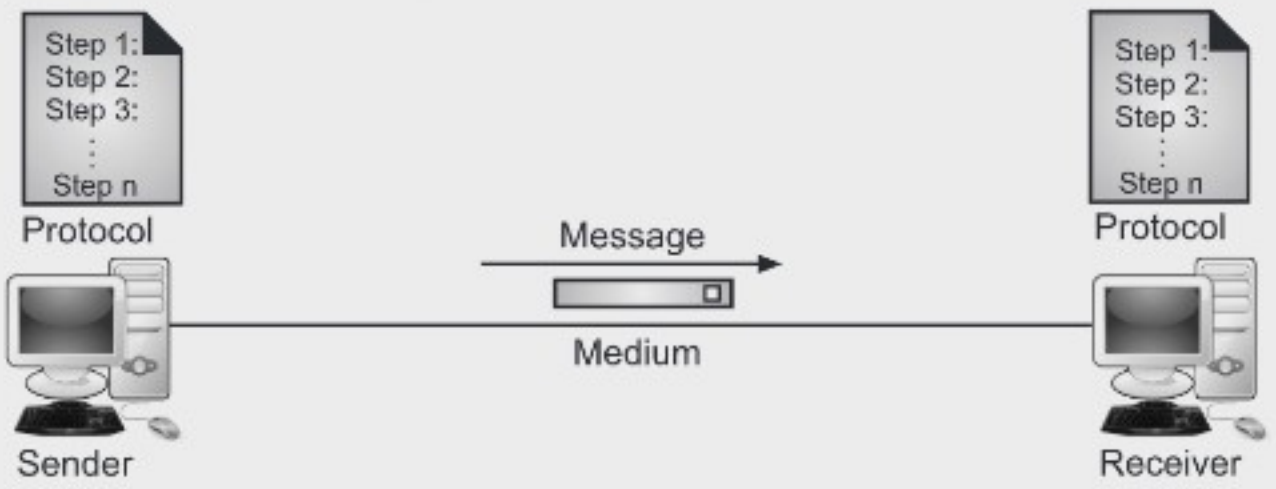


Fig. 1.1: Components of Data Communication System

- The five components data communication are explained below:
  1. **Sender:** It is the device that sends the data message. For examples: computer, workstation, video camera, telephone etc.

2. **Receiver:** It is the device that receives the data message. For examples: Computer, workstation, telephone, television etc.
3. **Message:** It is the information that includes text, numbers, pictures, audio and video to be communicated.
4. **Transmission Media:** It is the physical path by which the message travels from sender to receiver. The transmission media includes twisted pair wire, coaxial cable, fiber optic cable, and radio waves.
5. **Protocol:** It is a set of rules that governs data communication. Two devices may be connected but cannot communicate without protocol.

1.3 DATA REPRESENTATION (W-18)

- Data is collection of raw facts which is processed to deduce information. There may be different forms in which data may be represented.
- Today the information comes in different forms such as text, numbers, images, audio and video as explained below:

1. **Text:** Text in data communication, represented as a bit pattern, a sequence of bits i.e., 0's and 1's. Each set of bit pattern is called a code and the process of representing symbols is called coding. Coding system can be Unicode or ASCII. Text includes combinations of alphabets in small case as well as uppercase.
2. **Numbers:** It is also bit pattern, but not in ASCII. Numbers are directly converted into binary numbers to simplify mathematical operations. Numbers include combination of digits from 0 to 9.
3. **Images:** Images are also represented by bit patterns. An image is composed of matrix of pixels. The black and white image requires only 1 bit (0's and 1's) for one pixel. The gray image requires 8 bits for one pixel and color (RGB) image requires 24 bits for one pixel.
4. **Audio:** It refers to the recording or broadcasting of sound and music. It is continuous signal.
5. **Video:** It refers to the recording or broadcasting of picture or movie.

1.4 TYPES OF DATA FLOW – SIMPLEX, HALF DUPLEX, FULL DUPLEX

- In data communication the exchange of information takes place through transmission modes which defines the direction of the flow of information between two communication devices i.e., it tells the direction of signal flow between the two devices.
- Data communication between two devices occurs due to exchange of data in simplex, half duplex and full duplex transmission modes.

1. **Simplex:** In simplex data flow, information is sent only in one direction. In short, simplex mode data transmission is unidirectional (one way). For example, communication between a computer and a keyboard involves simplex data transmission.

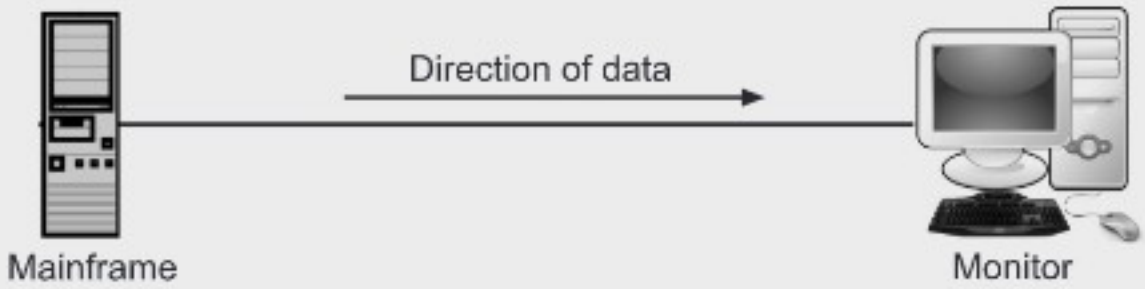


Fig. 1.2: Simplex Data Flow

2. **Half-duplex:** In half duplex data flow, data can be transmitted in both directions alternatively. Means each station can both transmit and receive, but not at the same time. It is also known as two-way alternate. For example, a walkie-talkie operates in half-duplex mode. It can only send or receive a transmission at any given time.

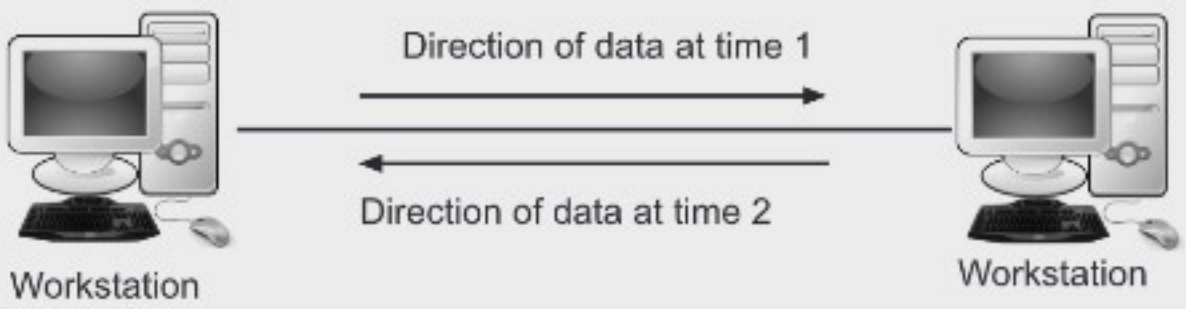


Fig. 1.3: Half-duplex Data Flow

3. **Full-duplex:** In full duplex data flow, data is transmitted in both directions at the same time. It is also known as two way simultaneous communication. For example, mobile phones operate in full-duplex mode when two persons talk on mobile phone, both can listen and speak simultaneously.

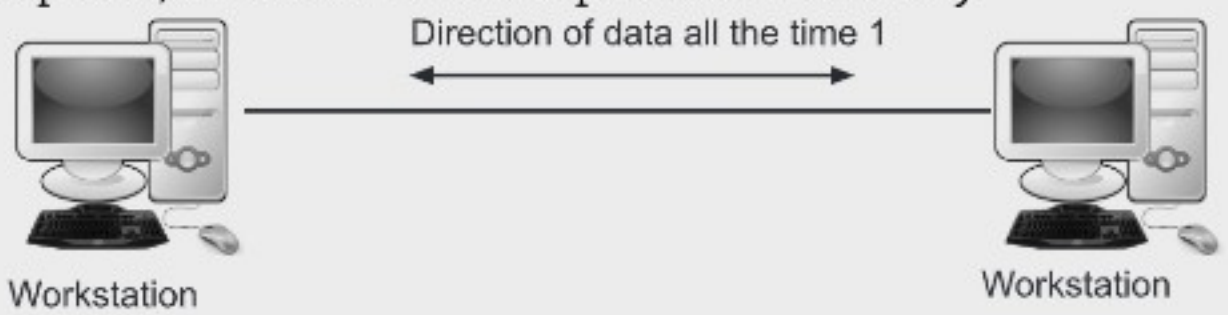


Fig. 1.4: Full-duplex Data Flow

1.5 COMPUTER NETWORKS

- A network is the interconnection of a set of computing devices capable of communication.
- A network is a set of devices often referred to as nodes like computer, printer, or any other device capable of sending and receiving data connected by media links as shown in Fig. 1.5.

- Computer network is a set or collection of computing devices that are linked to each other in order to communicate and share their resources with each other.

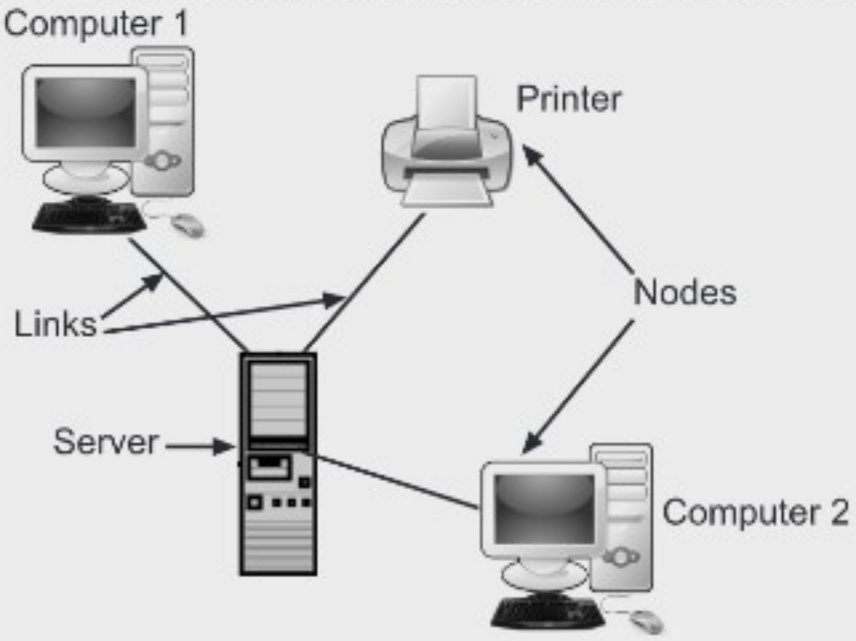


Fig. 1.5: Network Nodes and Links

- Computer network is divided into wired and wireless network. A wired network is simply a collection of nodes connected by cables like Ethernet, co-axial etc. A wireless network, which uses high-frequency radio waves to communicate between nodes.

1.5.1 Definition of Computer Network (S-19)

- The old model of a single computer serving all of the organization's computational need has been replaced by one in which a large number of separate but interconnected computers do the job. These systems are called Computer Network.

Definition:

- A computer network can be defined as "an interconnected collection of autonomous computers and computing devices". **OR**
- A computer network is "an interconnection of computers and computing equipments like printers etc. using either wires or radio waves (wireless) made to share hardware and software resources".
- Fig 1.6 shows a typical computer network.

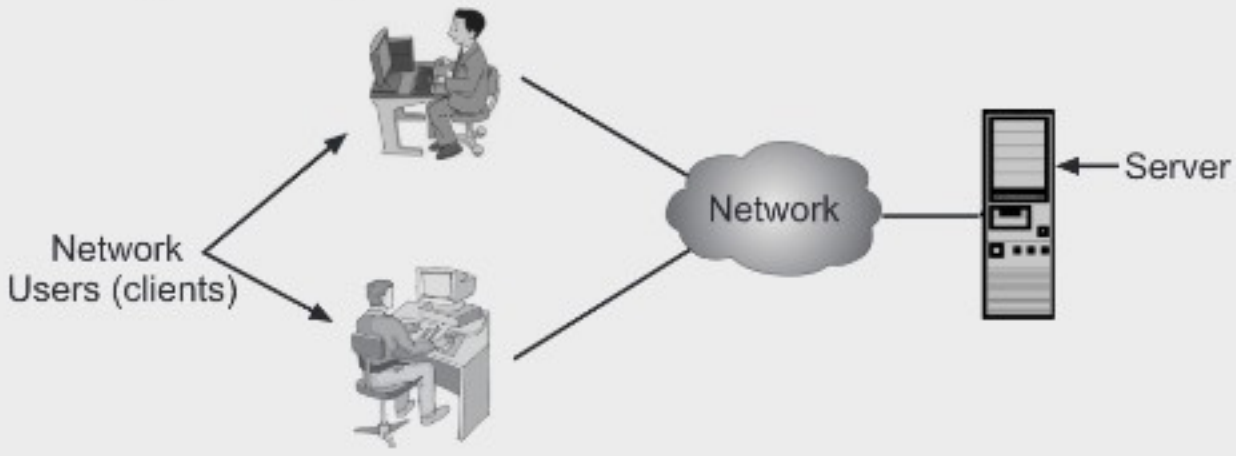


Fig. 1.6: Typical Computer Network

1.5.2 Goals of Computer Network (W-18)

- The computer networks are playing an important role in providing services to large or small or medium organizations as well as to the individual common man.
- Network services are the things that a network can do.
- Like human being computer network provides following goals:

1. **Resource Sharing:**

- It is the main goal of the computer network. The goal is to provide data and hardware to all programs on network regardless of physical location of resources and users.
- In short, to provide sharing of resources such as information or processors.

2. **High Reliability:**

- Network provides high reliability by having alternative sources of data.
- For example, all files could be replicated on more than one machines, so if one of them is unavailable due to hardware failure or any other reason, the other copies can be used.

3. **Minimize Cost:**

- Small computers have a much better price to performance ratio as compared to large ones. So it is always minimizing the cost to set up a network of large small number of computers than the large ones.
- As well as by sharing the resources like printer, we can save the cost. While designing cost of a network is an important factor.

4. **High Performance:**

- Computer network provides the network user with maximum performance at minimum cost. The network performance can be measured by its transit time and response time.
  (i) Transit time is the amount of time required for a message to travel from one device to another device in network.
  (ii) Response time is the time elapsed between an inquiry and a response.
- Network performance depends on a number of factors including, network transmission medium, network hardware, network software and traffic load. Computer network have provided means to increase system performance as the work load increases.

5. **Scalability:**

- We can easily extend computer network just by adding more computers, printers or any other devices without disturbing others and affecting overall performance.

6. **Powerful Communication Medium:**

- A computer network provides a powerful communication medium.

- Computer network helps people who live or work apart to report together. So, when one user prepared some documentation, he/she can make the document online enabling other to read and convey their opinions. For this reason, computer network is a powerful communication medium.

7. **Distribution of Workload:**

- By using computer network, large work can be distributed among different network users.

8. **Security:**

- Network security issues comprise of prevention from virus attacks and protecting data from unauthorized access. Only authorized user can access resource in a computer network.

1.5.3 Applications of Computer Network

- Nowadays, computer network has become an essential part of Industry, Entertainment world, Business as well as our daily lives.
- Some of the applications of a computer network in different fields are, Business applications, Home applications, Mobile user etc., as discussed below.

1.5.3.1 Business Applications

- Business applications are built based on the requirements from the business users. Also, these business applications use certain kind of Business transactions or data items.
- Network allows users to share both hardware and software resources, increasing efficiency and facilitating workplace collaboration. Computer networks are being used in almost all business processes.
- In a networked environment, each computer on a network may access and use hardware resources on the network, such as printing a document on a shared network printer.
- The capability of providing access to data and information on shared storage devices is an important feature of many networks. Users connected to a network may run application programs on remote computers.

1. **Resource Sharing:**

- One of the most important business application of computer network is resource sharing. This enables all programs, equipments and data available to anyone on the network regardless of the physical location of the user and the resource.

2. **Powerful Communication Medium:**

- A computer network provides a powerful communication medium among widely separated employees in Business. Employees in a business can use e-mail for daily communication.

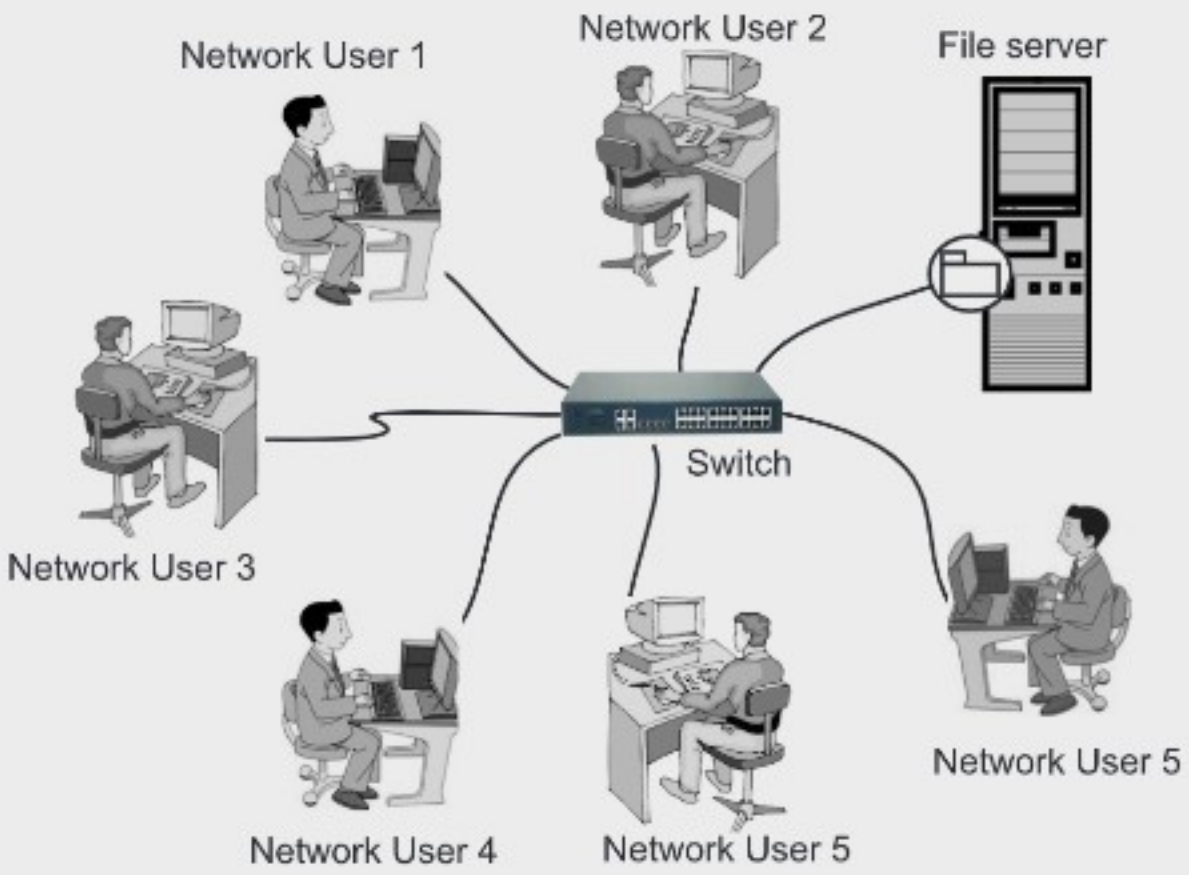


Fig. 1.7: Communication using Computer Network

- Using network it is easy for two or more employees, who are separated by geographical locations to work on a report, document or R and D simultaneously i.e. on line.
- Fig. 1.7 shows network which allows Employees to communicate using e-mail, newsgroups, and video conferencing etc.
- Videoconferencing also very helpful in business which enables employees from different locations to do virtual meetings, seeing and hearing each other and even writing on a shared virtual blackboard. Videoconferencing is a powerful tool for eliminating cost and time required for traveling.

3. **Electronically Business:**

- Using computer networks organizations/companies can do business electronically with other organizations/companies, suppliers and customers which not only saves time and cost but also reduces the need for large inventories and enhances efficiency.

4. **E-commerce:**

- The last application is growing more important is doing business with consumers over the Internet i.e. E-commerce.
- E-commerce is trading in products or services using computer networks, such as the Internet.
- E-commerce businesses may employ on online shopping, online banks, Electronic Data Interchange (EDI), online Business-to-business buying and selling and so on.

1.5.3.2 Home Applications

- Starting in 1990s, the computer networks began to start delivering services to the private individuals at home.
- Some of the most popular uses of the network for home users are Access to remote information are Person to Person Communication, Interactive entertainment and Electronic Commerce etc., as discussed below.

1. Access to Remote Information:

- Remote access refers to connection to a data processing system from a remote location.
- Remote access is the ability to get access to a computer or a network from a remote distance. For examples, Home users get access to the Internet through remote access to an Internet Service Provider (ISP).
- Access to remote information involves interaction· between a person and a remote database.

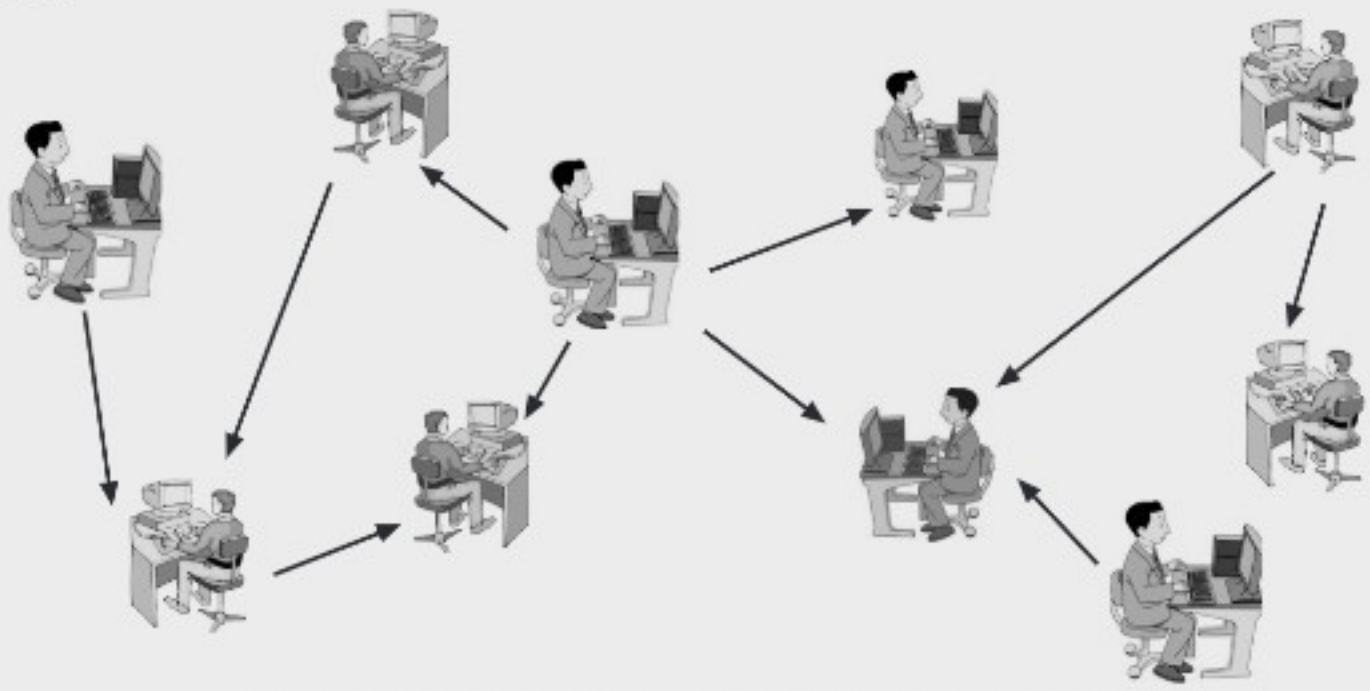


Fig. 1.8: Remote Access using Computer Network

- Access to remote information occurs in many forms like:
  - (i) Home shopping, paying telephone, electricity bills, e-banking, online share market etc.
  - (ii) Newspaper is online and is personalized, digital library consisting of books, magazines, scientific journals etc.
  - (iii) World Wide Web (WWW) which contains information about the arts, business, cooking, government, health, history, hobbies, recreation, science, sports etc.

2. Person to Person Communication:

- Communication is the act of transferring information through verbal messages, the written word, or more subtle, non-verbal signals.

- Person to person communication includes:
  - (i) **Electronic-mail (e-mail):** In person to person communication Email is used on a daily basis by millions of people all over the world.
  - (ii) **Chatting or Instant Messaging:** It can also be used for communication. Not only text but also audio, video can be exchanged in real time.
  - (iii) **Real time e-mail i.e. Video Conferencing:** It allows remote users to communicate with no delay by seeing and hearing each other. Video conferencing is being used for remote school, getting medical opinion from distant specialists etc.
  - (iv) **World-wide Newsgroups:** In which one person posts a message and all other subscribers to the newsgroup can read it or give their feedbacks.

3. **Interactive Entertainment:**

- Entertainment is a huge and growing industry. These days we can see many live programmes and shows. The best thing is that we can interact with them by participating in the quizzes and the contests organized by them.
- In future, it may be possible to select any movie or television program ever made, in any country and have it displayed on your screen instantly. New films may become interactive. Live television may also become interactive.
- Another application may be game playing. If games are played with goggles and three dimensional real time, photographic quality moving images, we have a kind of worldwide shared virtual reality.

4. **E-commerce:**

- E-commerce facilitates home shopping, catalogs of company products, online technical support.
- E-commerce also popularly employed for bills payments, banking, investments, online auctions.
- Commonly used forms of e-commerce and their typical applications are shown below:
  - (i) **B2C (Business-to-Consumer):** Ordering books online.
  - (ii) **B2B (Business-to-Business):** Car manufacture ordering tires from supplier.
  - (iii) **G2C (Government-to-Consumer):** Government distributing tax forms electronically.
  - (iv) **C2C (Consumer-to-Consumer):** Auctioning second hand products online.
  - (v) **P2P (Peer-to-Peer):** File sharing.

1.5.3.3 Mobile Users

- Mobile computers, such as notebook computers and Personal Digital Assistants (PDAs), are one of the fastest growing segments of the computer industry.

- Many owners (users) of these computers have desktop machines back at the office and want to be connected to their home base even when away from home or on route.
- Since, having a wired connection is impossible in cars and airplanes. So the importance of wireless networks. Wireless networks are either fixed wireless or mobile wireless.
- There are various applications of mobile wireless systems. Users can access to home networks, other information, m-commerce, inventory tracking systems, location dependent services, mobile maps, emergency services, mobile banking, money transfer etc.

1.5.3.4 Some other Applications of Computer Networks

1. **Banking:**

- Computers are instrumental to the way the banking industry performs its business. This technology allows banks to be able to take banking transactions and update accounts in real time.
- Financial services: It include credit history searches, foreign exchange and investment services and Electronic Fund Transfer (EFT), which allow a user to transfer money without going to bank.

2. **Insurance:**

- The world of insurance relies on computers to the same extent as banks.
- With the use of the Internet, insurance companies are able to access information which will determine whether they accept clients or not.

3. **Marketing and Sales:**

- Marketing professional uses them to collect exchange and analyze data relating to customer needs and product development cycles. Sales application includes Teleshopping, which uses order entry computers or telephone connected to an order processing network, and online reservation services for railways, hotels, airlines, restaurants theatre etc.

4. **Financial Services:**

- It include credit history searches, foreign exchange and investment services and Electronic Fund Transfer (EFT), which allow a user to transfer money without going to bank.

5. **Manufacturing:**

- Computer networks are used today in many aspects of manufacturing, including the manufacturing processes itself. Two aspects that uses network to provide essential services are Computer Assisted Design (CAD) and Computer Assisted Manufacturing (CAM), both of which allow multiple user to work on a project simultaneously.

6. **Electronic Data Exchange (EDI):**

- EDI allows business information (including documents such as purchase orders and services) to be transferred without using paper.

1.5.4 Advantages and Disadvantages of Computer Network

- The ability to exchange data and communicate efficiently is the main purpose of networking computers.

Advantages: **(S-18)**

1. **Easy Communication:** It is very easy to communicate through a network. People can communicate efficiently using a network with a group of people. They can enjoy the benefit of emails, instant messaging, telephony, video conferencing, chat rooms, etc.
2. **Ability to Share Files, Data and Information:** This is one of the major advantages of networking computers. People can find and share information and data because of networking. This is beneficial for large organizations to maintain their data in an organized manner and facilitate access for desired people.
3. **Flexible Access:** Access of files from computers throughout the world, and 24 × 7 environment.
4. **Workgroup Computing:** Workgroup software (such as Microsoft BackOffice) allows many users to work on a document or project concurrently.
5. **Sharing Hardware:** Another important advantage of networking is the ability to share hardware. For an example, a printer can be shared among the users in a network so that there's no need to have individual printers for each and every computer in the company. This will significantly reduce the cost of purchasing hardware.
6. **Centralized Software Management:** Software can be loaded on one computer (the file server) eliminating that need to spend time and energy installing updates and tracking files on independent computers throughout.
7. **Sharing Software:** Users can share software within the network easily. Networkable versions of software are available at considerable savings compared to individually licensed version of the same software. Therefore large companies can reduce the cost of buying software by networking their computers.
8. **Security:** Sensitive files and programs on a network can be password protected. Then those files can only be accessed by the authorized users. This is another important advantage of networking when there are concerns about security issues. Also each and every user has their own set of privileges to prevent those accessing restricted files and programs.

9. **Speed:** Sharing and transferring files within networks is very rapid (fast), depending on the type of network. This will save time while maintaining the integrity of files.

Disadvantages:

1. **Expensive to Build:** Building a network is a serious business in many occasions, especially for large scale organizations. Cables and other hardware are very costly to buy and replace.
2. **Security Threats:** Security threats are always problems with large networks. There are hackers who are trying to steal valuable data of large companies for their own benefit. So it is necessary to take utmost care to facilitate the required security measures.
3. **Bandwidth Issues:** In a network there are users who consume a lot more bandwidth than others. Because of this some other people may experience difficulties.
4. **Lack of Robustness:** If the main file server of a computer network breaks down, the entire system becomes down and useless.
5. **Needs an Efficient Handler:** The technical skills and knowledge required to operate and administer a computer network.
6. **Breakdowns and Possible Loss of Resources:** One major disadvantage of networking is the breakdown of the whole network due to an issue of the server.

1.6 NETWORK HARDWARE

- Network hardware/structure is a design required for developing any computer network.
- For classification of computer network transmission technology is important.
- Transmission technology refers how two devices are connected and how they are communicating. n transmission technology 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.
- The transmission technology can be broadly categorized into two types:
  1. Point-to-point networks, and
  2. Broadcast networks (multipoint)

1.6.1 Point-to-Point Network (W-18)

- Communication between two directly interconnected devices is referred to as point-to-point communication.

- A point-to-point connection provides a dedicated link between two devices as shown in Fig. 1.9.

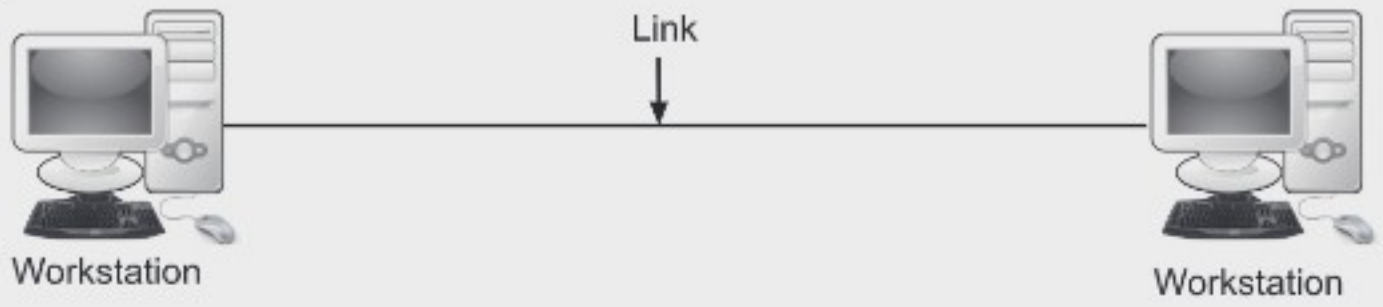


Fig. 1.9: Point-to-Point Connection

- Point-to-point networks consist of many connections between individual pairs or machines. On such type of network, when any packet is sent from source to destination, it may have to first visit one or more intermediate machines.
- In such type of networks often multiple routes of different lengths are possible.
- Smaller networks tends to use broadcasting, whereas larger networks usually are point to point.
- A point to point network with one sender and one receiver is sometimes called unicasting.
- Examples of point-to-point networks are LAN (Local Area Networks), MAN (Metropolitan Area Network), WAN (Wide Area Network), Internet, etc.

Advantages:

1. **Simple:** A point-to-point network is one of the simplest networks because it only involves two nodes.
2. **Cheapest and effective:** This is one of the cheapest and most effective network architectures because it doesn't involve the cost of redundancies.
3. **Less Complex:** It does not add the complexity of needing several nodes functioning to make a connection.

Disadvantages:

1. **More expensive:** As it requires lots of transmission lines and switching elements to connect remote hosts.
2. **Impractical from:** The point-point network is impractical from a networking standpoint because rarely is only one connection between two nodes adequate.

1.6.2 Broadcast Network

- The networks having multipoint configuration are called as Broadcast Network.
- A broadcast network have a single communication channel that is shared by all the machines on the network.
- Packets sent by any machine are received by all the others. The address field within the packet specifies the intended recipient.

- After receiving a packet, a machine checks the address field. If packet is intended for the receiving machine, that machine processes the packet, if packet is intended for some other machine, it is just discarded.
- Broadcast network supports two modes of operations:
  1. **Broadcasting:** Broadcast systems generally use a special code in the address field for addressing a packet to all the concerned computers. When a packet with this code is transmitted, it is received and processed by every machine on the network. This mode of operation is called broadcasting.
  2. **Multicasting:** Some broadcast systems also support transmission to a subset of the machines known as multicasting. When a packet is sent to a certain group, it is delivered to all machines of that group. Examples of this network is Ethernet and Bus topology based on LAN.
- Fig. 1.10 shows a broadcast network.

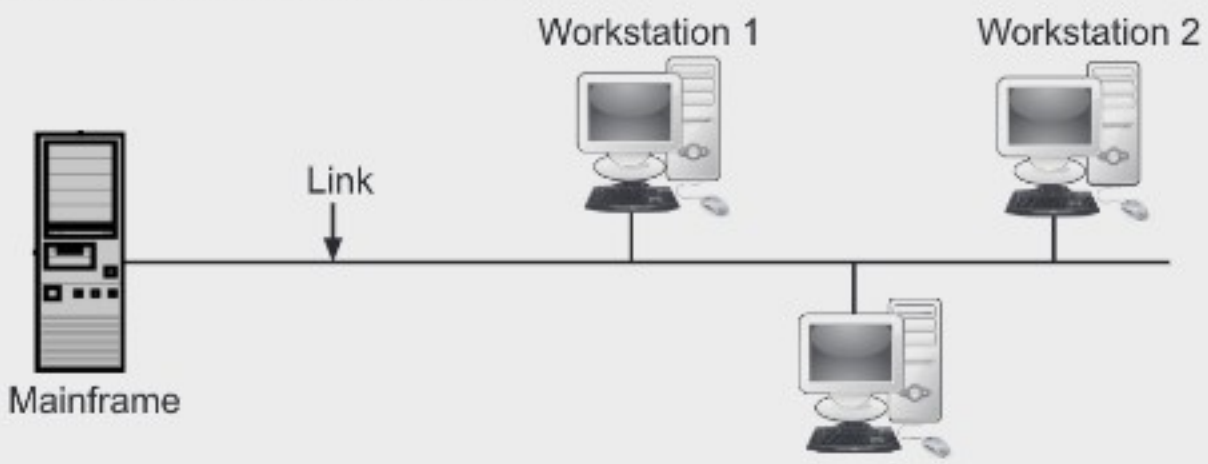


Fig. 1.10: Broadcast Network

Table 1.1: Comparison between Point-to-Point and Broadcast Networks **(W-18)**

Sr. No.	Point-to-Point Network	Broadcast Network
1.	Point-to-point network has more than one communication channel.	Broadcast network has single communication channel.
2.	Point-to-point network is a connection of routers.	Broadcast network is a connection of host and repeaters.
3.	Limited number of concurrent connection.	Unlimited number of concurrent connection.
4.	It does not require extra cost to setup network.	It requires extra cast to set up network.
5.	Point-to-point Network provides security and privacy because communication channel is not shared.	Broadcast network does not provides security and privacy because communication channel is shared.

1.7 NETWORK TOPOLOGIES

- The word "topology" comes from topos, which is Greek word for "place." The term topology refers to the way in which a network is laid out physically.
- Two or more devices connect to link, two or more links form a topology.
- Network topology defines the geographic arrangement of computer networking devices.
- Topology describes the actual layout of the computer network hardware.
- Topology defines the physical or logical arrangement of links in a network.
  1. **Physical Topology:** A physical topology describes the placement of network nodes and the physical connections between them. This includes the arrangement and location of network nodes and how they are connected.
  2. **Logical Topology:** It refers to the paths that messages take to get from one place on the network to another place.

Definition of Topology **(S-18)**

- The "way of connecting the computers in a network is called as topology".

OR

- The topology of a network is "the geometric arrangement of the relationship of all the links and linking devices (nodes) in a network".

1.7.1 Types of Topologies (S-19)

- The different types of network layouts are shown in Fig. 1.11.

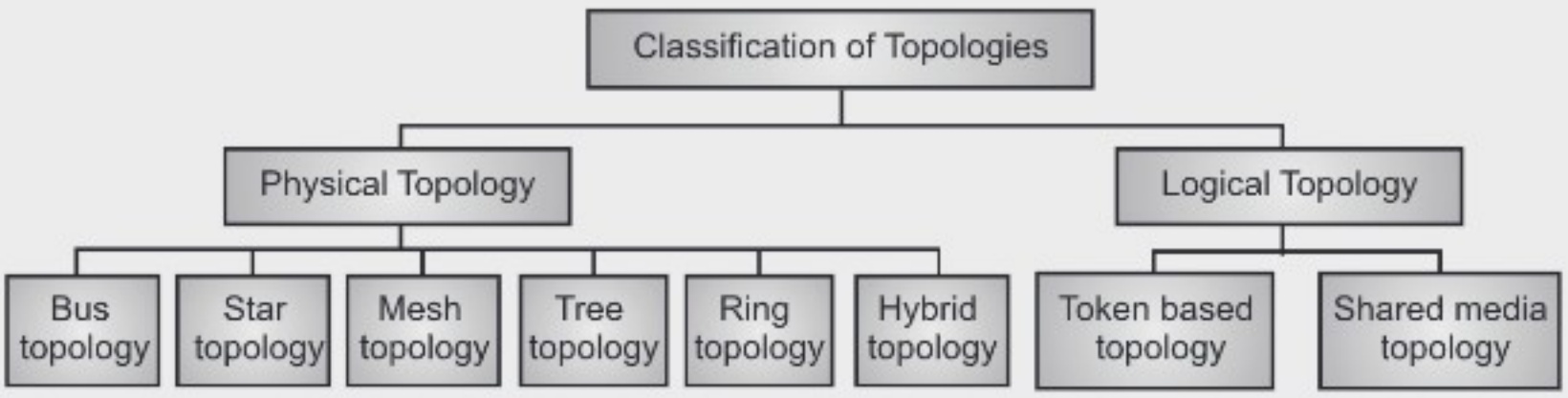


Fig. 1.11: Types of Topologies in Computer Network

1.7.1.1 Bus Topologies (S-19)

- In bus topology, all nodes are connected to a central cable which is called a bus. This bus is also called as a Trunk or sometimes it is also referred to as Backbone cable.
- Trunk cable is then connected to the branch cables which were further connected to the PCs. Every network device communicates with the other device through this Bus.
- Nodes are connected to the bus cable by drop lines and taps. A drop line is a connection running between the device and the main cable.

- A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core.
- A node (computer) that wants to send data, it puts the data on the bus which carries it to the destination node.
- When one computer sends a signal on the wire, all the computers on the network receive the information, but only one accepts the information. The rest regrets the message. One computer can send a message at a time. A computer must wait until the bus is free before it can transmit.
- Fig. 1.12 shows a bus topology or network.

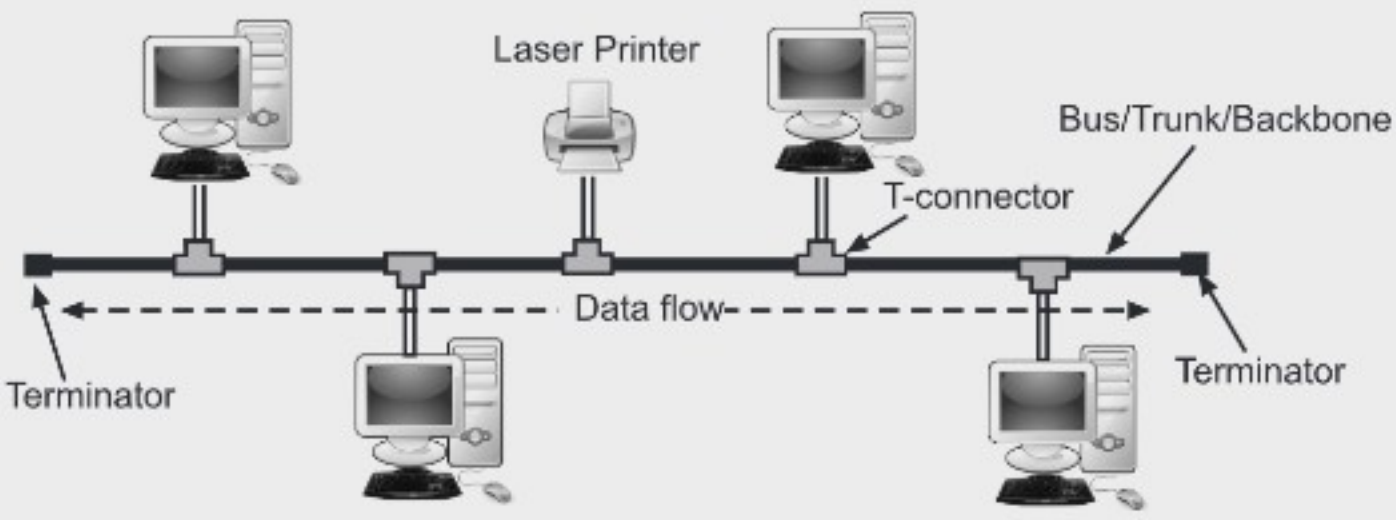


Fig. 1.12: Bus Topology

Advantages:

1. Easy to install and setup.
2. Requires less cabling length than Mesh and Star so cheaper in cost.
3. Fast as compare to ring topology.
4. Sufficient for small network.

Disadvantages:

1. It can not connect a large number of computers.
2. A fault or break in the bus cable stops all transmission.
3. Difficult to identify the problem if the entire network shuts down.
4. Collision may occur.
5. Heavy network traffic can slow a bus considerably.
6. Used for only small network.

1.7.1.2 Ring Topologies

- In ring topology, the computers in the network are connected in a circular fashion which form of a ring.
- In ring topology, each computer is connected to the next computer, with the last one connected to the first, or we can say each device is connected to other two devices

with dedicated link in one direction, from device to device. Each computer in the ring incorporates a repeater.

- When a computer receives a signal intended for another computer, its repeater regenerates the bits and passes them. The message flow around the ring in one direction. Today higher speed LANs has made this topology less popular.
- Fig. 1.13 shows a ring topology.

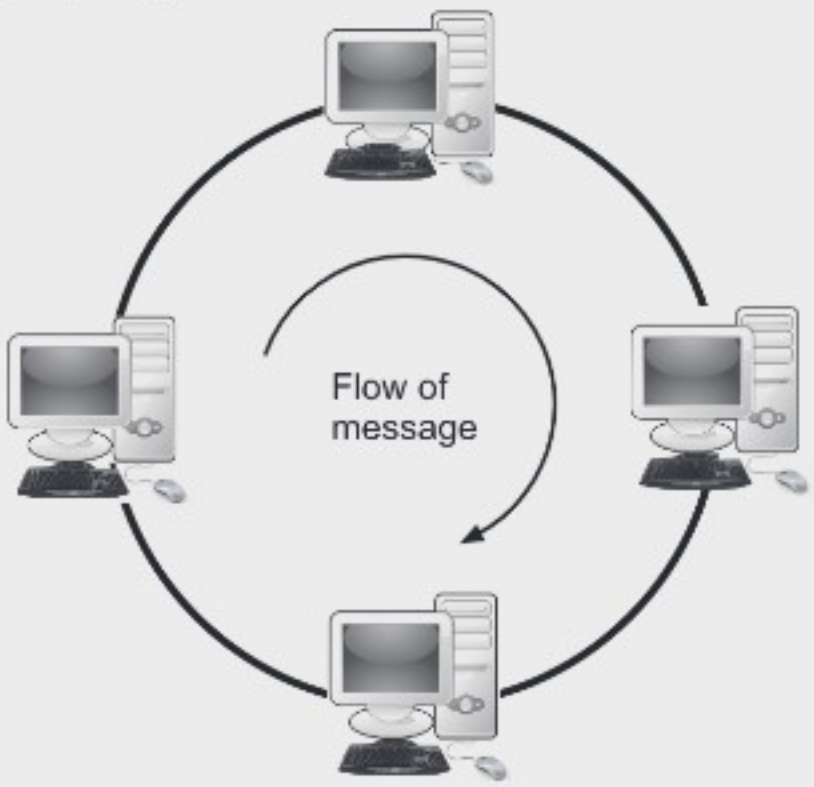


Fig. 1.13: Ring Topology

Advantages:

1. Require less cabling.
2. Less expensive and easy to install.
3. Adding or deleting a device is easy.
4. Reduces chances of collision.
5. Each computer has equal access to resources.
6. There is no need for network server to control the connectivity between workstations.
7. It's performance is better than that of Bus topology.
8. Fault isolation is simplified.

Disadvantages:

1. If one node goes down, it takes down the whole network.
2. Slow in speed.
3. Reconfiguration is needed to add one node, whole network must be down first.
4. Traffic is unidirectional.
5. Network is highly dependent on the wire which connects different components.

1.7.1.3 Star Topologies (S-18)

- In star topology each device has a dedicated point-to-point link on it to a central controller, usually called hub or switch. The devices are not directly connected to one another.
- Each computer on a star network first communicates with a central hub/switch that forwards the message either to all the computers or only to the destination computers.
- Communication is controlled by central controller (Hub/Switch) only.
- Star topology is generally used in LANs. Fig. 1.14 shows a star topology or network.

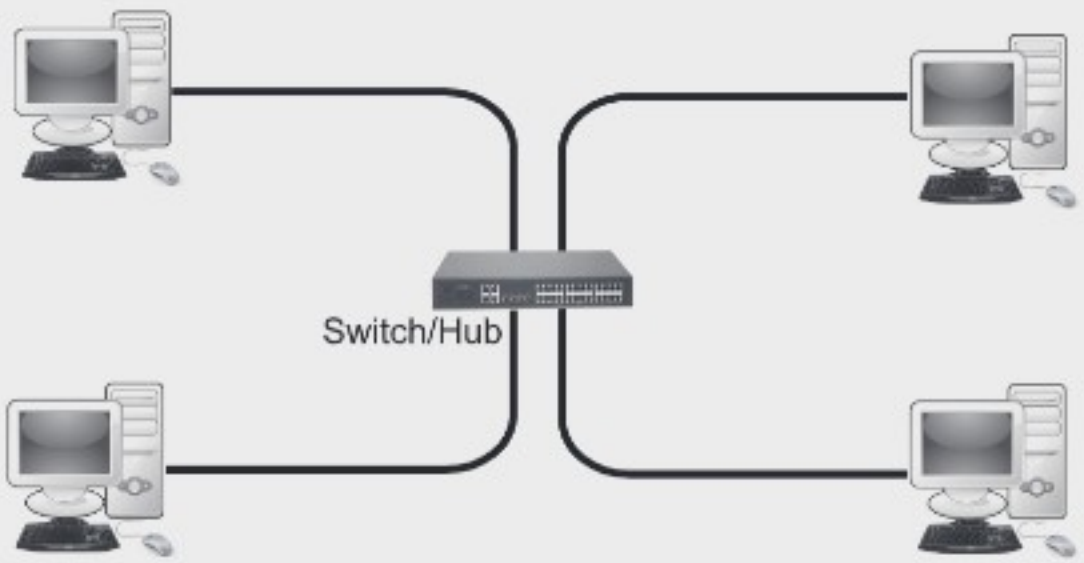


Fig. 1.14: Star Topology

Advantages:

1. Easy to install, reconfigure and wire.
2. Centralized management which helps in monitoring the network.
3. Robustness i.e., if one link fails, only that link is affected.
4. Fast as compare to ring topology.
5. Multiple devices can transfer data without collision.
6. Eliminates traffic problem.
7. No disruptions to the network then connecting or removing devices.
8. It is easy to detect the failure and troubleshoot it.

Disadvantages:

1. If central node (hub or switch) goes down then entire network goes down.
2. More cabling is required than bus or ring topology, so more expensive.
3. Performance is depended on capacity of central device.

1.7.1.4 Mesh Topologies

- In a mesh network topology, each of the network node, computer and other devices, are interconnected with one another with dedicated point to point link.

- Dedicated means that link carries traffic only between the two devices it connects. So for N number of nodes, there will be total n(n-1)/2 links require.
- Mesh topology is usually implemented in a limited fashion, as a backbone connecting the main computers of a hybrid network that can include several other topologies.
- Fig. 1.15 shows a mesh topology. Mesh topology is used in WAN.

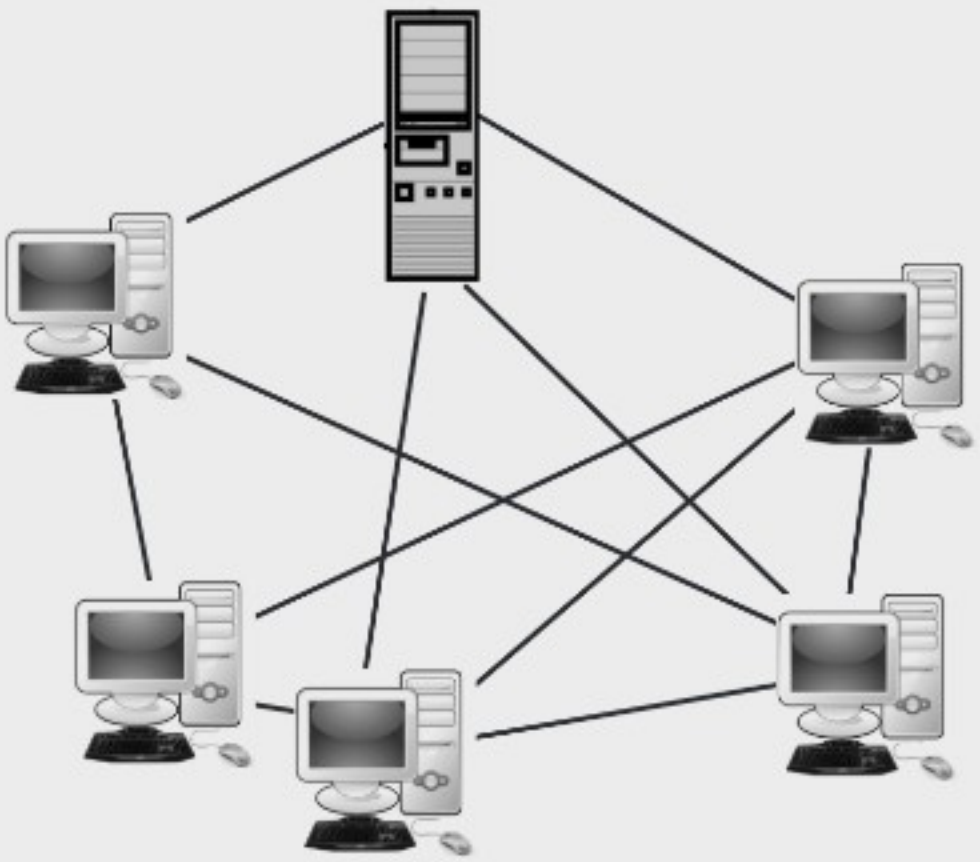


Fig. 1.15: Mesh Topology

Advantages:

1. Each connection can carry its own data load due to dedicated link.
2. Eliminates traffic problem.
3. Mesh topology is robust. If one link becomes unusable, it does not affect other systems.
4. Privacy or security because of dedicated line.
5. Point-to-point link make fault identification easy and simple.

Disadvantages:

1. More cables are required than other topologies.
2. Overall cost of this network is very high.
3. Installation and reconfiguration is very difficult.
4. Setup and maintenance of this topology is very difficult.
5. Expensive due to hardware requirements such as cables.

1.7.2 Comparison between Bus, Ring and Star Topologies

Table 1.2: Comparison between Bus, Ring and Star Topologies

Terms	Bus Topology	Ring Topology	Star Topology
1. Structure	There is a single central cable (backbone) and all computers and other devise connect to it.	All computers and other devices are connected in a circle or ring.	There is a central host (hub/switch) and all node connect to it.
2. Host existence	Depends on network needs.	Depends on network needs.	Yes.
3. Connection between nodes	It has no connection between the nodes.	Yes.	No.
4. Host failure	Network can still run.	Network will fail.	Network will fail.
5. Ease of trouble-shooting	Difficult, need to search for the problematic node one by one.	Depends on backbone. If there is backbone, trouble-shooting is difficult. If there is not backbone, the focus is one the two nodes not communicating.	Depends on the host. It is easier to repair the problematic host. However, if the nodes fail, then each node has to be searched.
6. Ease of adding or removing nodes	Easy.	Difficult.	Average.
7. Number of nodes when extending network	Many.	Limited.	Limited.

1.8 NETWORK TYPES

- Computer networks fall into three classes regarding the size, distance and the structure namely LAN (Local Area Network), MAN (Metropolitan Area Network), WAN (Wide Area Network), as shown in Fig. 1.16.

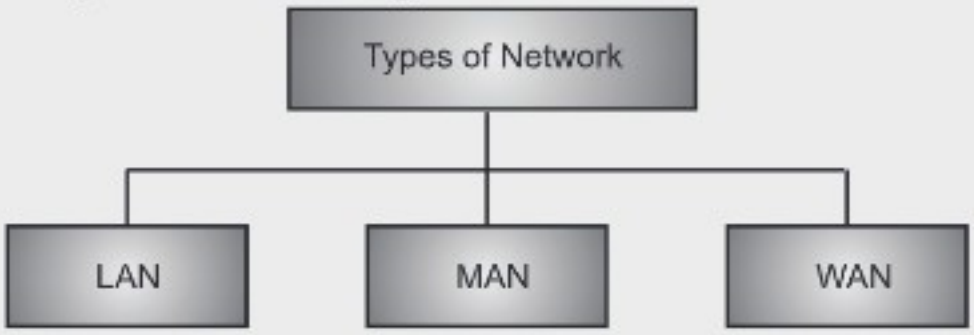


Fig. 1.16: Types of Computer Network

- Fig. 1.17 shows geographical arrangement of LAN, WAN and MAN.

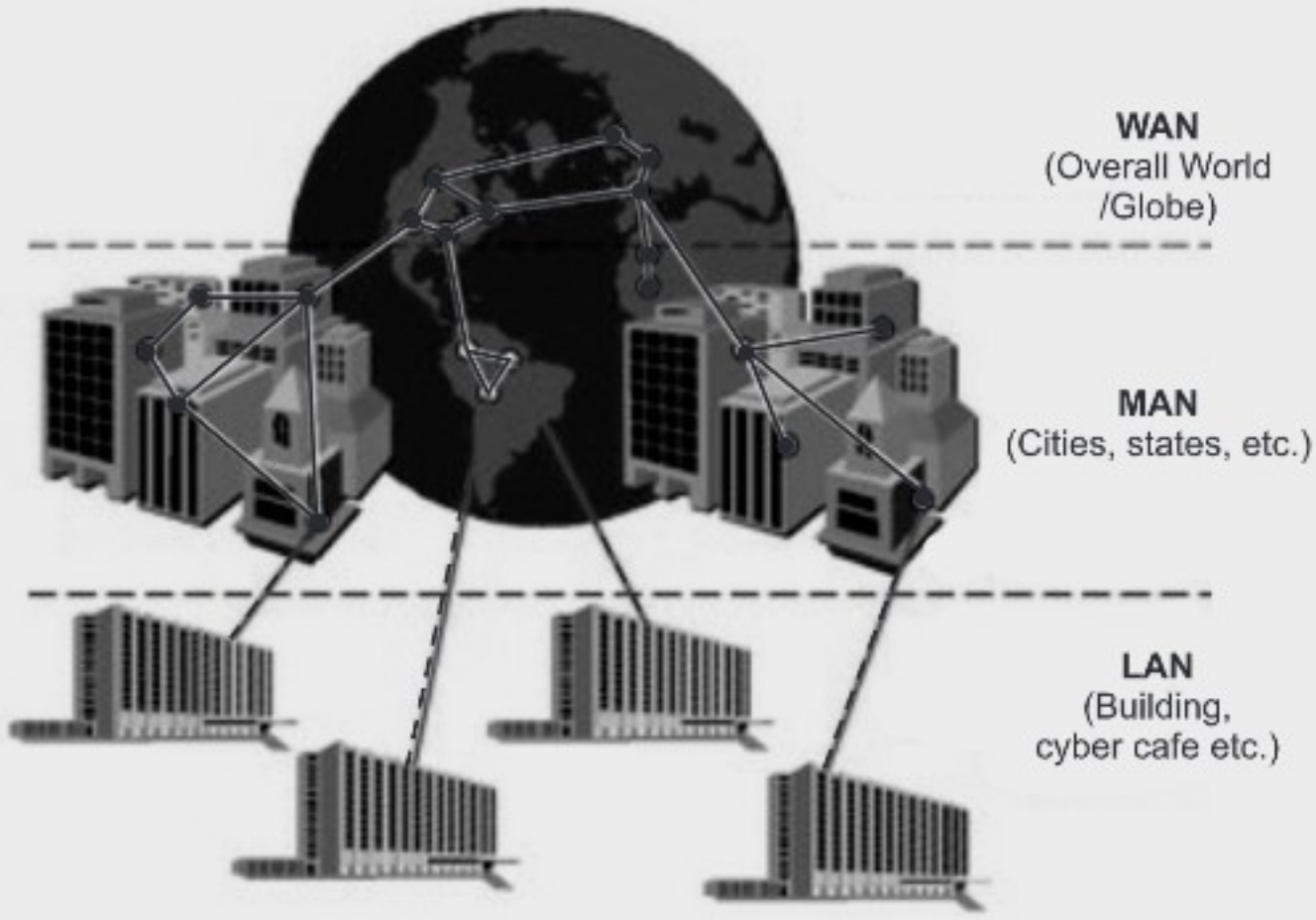
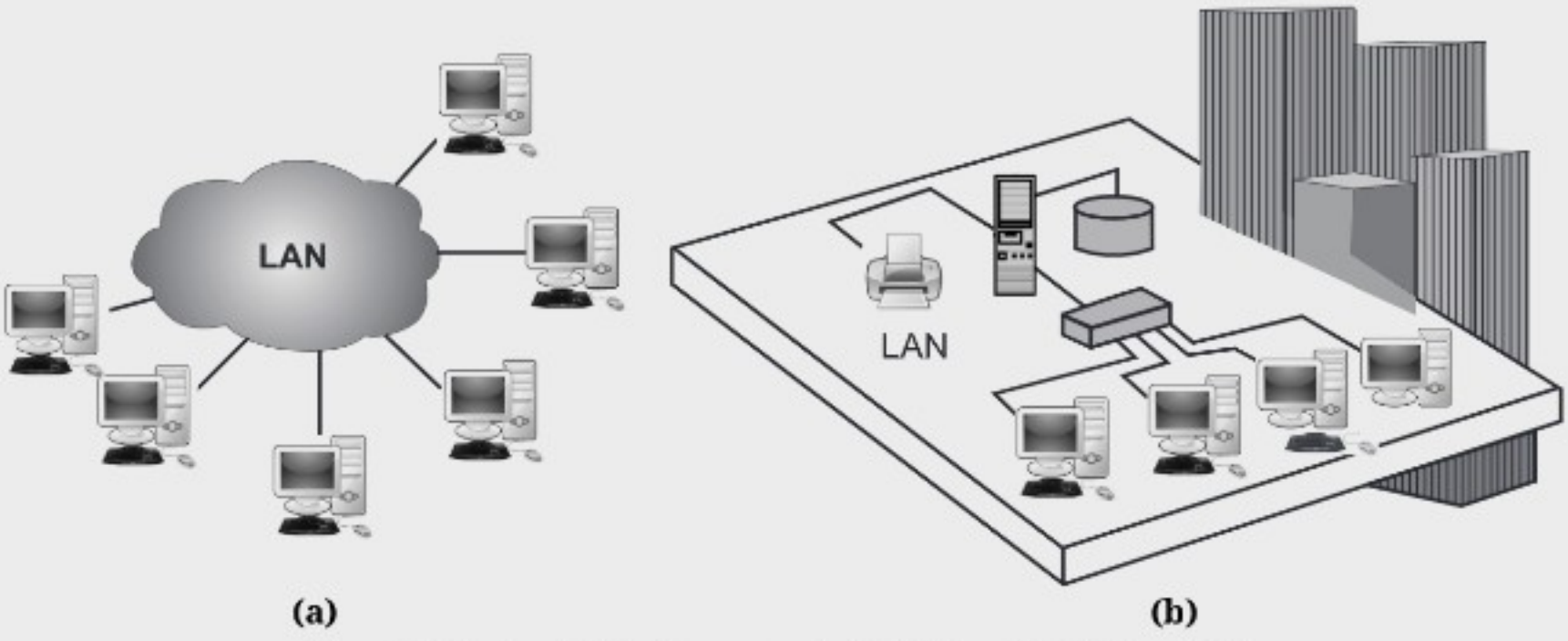


Fig. 1.17: Geographical arrangement of LAN, WAN and MAN

1.8.1 Local Area Network (LAN)

- Local area networks are privately-owned networks covering a small geographical area, (less than 1 km) like a home, office, or groups of buildings.
- Depending on the needs of the organization and the type of technology used, a LAN can be as simple as two PCs and a printer or it can extend throughout a organization.
- LANs are widely used to connect personal computers and workstations to share resources like printers and exchange information.
- LANs are distinguished from other kind of networks by three characteristics i.e., their size, their transmission technology and their topology.
- Generally, LAN will use only one type of transmission medium wired or wireless. The most common LAN topologies are bus, ring or star.
- Early LAN had data rates in the 4 to 16 mbps range. Today, speeds are normally 100 to 1000 mbps. Wireless LANs are the newest evolution in LAN technology.
- Nowadays, LANs are being installed using wireless technologies. Such a system makes use of access point or APs to transmit and receive data. One of the computers in a network can become a server serving all the remaining computers called clients.
- For example, a library will have a wired or wireless LAN network for users to interconnect local networking devices. For examples, printers and servers to connect to the Internet.

- Fig. 1.18 (a) shows a typical LAN while Fig. 1.18 (b) shows a building LAN.



(a) (b)

Fig. 1.18: (a) and (b) shows typical LAN and building LAN

Characteristics of LAN:

1. Every computer has the potential to communicate with any other computers of the network.
2. High degree of interconnection between computers.
3. Easy physical connection of computers in a network.
4. Inexpensive medium of data transmission.
5. High data transmission rate.

Advantages of LAN:

1. The reliability of LAN is high because the failure of one computer in the network does not effect the functioning for other computers.
2. Addition of new computer to network is easy and simple.
3. High rate of data transmission is possible.
4. Peripheral devices like magnetic disk, printer etc. can be shared by other computers.
5. Less expensive to install.

Disadvantages of LAN:

1. Used for small geographical areas (less than 1 km).
2. Limited computers are connected in LAN.
3. Special security measures are needed to stop users from using programs and data that they should not have access to network.
4. LAN need to be maintained by skilled technicians.
5. In LAN if the file server develops a serious fault, all the users are affected.

1.8.2 Metropolitan Area Network (MAN)

- If a network spanning a physical area larger than a LAN but smaller than a WAN, such as a city then this network is called Metropolitan Area Network (MAN).
- MAN is an extended face of LAN, in which computing devices spread over a city are interconnected with communication mediums to form a network.
- Geographical area for MAN lies between 16 km to 50 km generally covers towns and cities. In this type of networks data is transmitted over one or two cables.

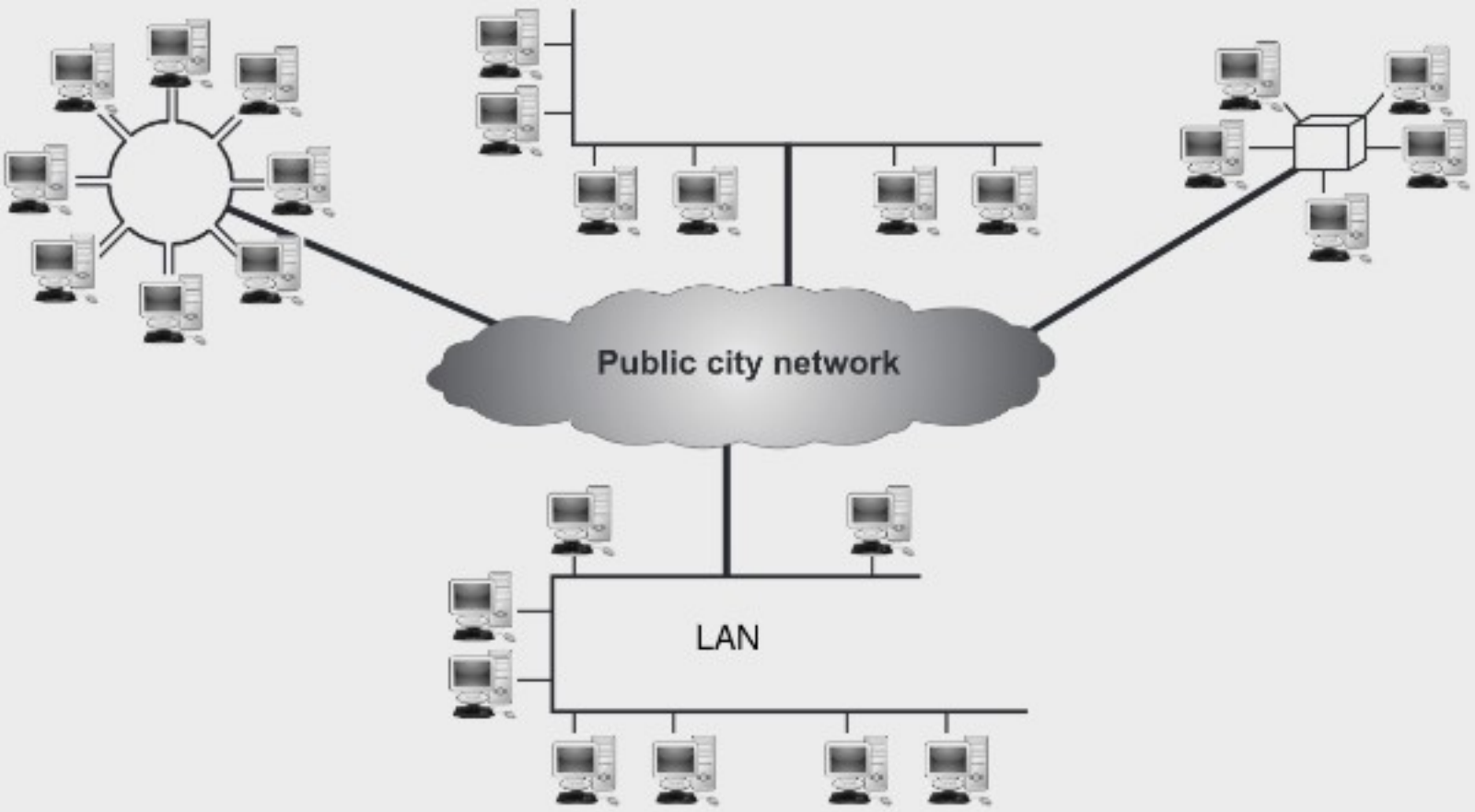


Fig. 1.19: MAN

- MAN can be owned by one private organization or public service company such as local telephone or cable television company.
- By interconnecting smaller networks within a large geographic area, information is easily disseminated throughout the network. Local libraries and government agencies often use a MAN to connect to citizens and private industries. ATM (Asynchronous Transfer Modes) FDDI (Fiber Distributed Data Interface) etc. are the technologies is used in MAN.

Advantages:

1. MAN spans large geographical area than LAN.
2. MAN falls in between the LAN and WAN therefore, increases the efficiency of handling data.
3. MAN saves the cost and time attached to establish a wide area network.
4. MAN offers centralized management of data.
5. MAN enables us to connect many fast LANs together.

Disadvantages:

1. Cost is high.
2. Speed is slow.

1.8.3 Wide Area Network (WAN) (S-19)

- WAN is a computer network used to connect different equipments from remote areas.
- A WAN provides long distance transmission of data, voice image and video information over large geographical areas that may comprise a country, a continent or even the whole world.
- It contains collection of machines intended for running users programs. These machines are called as hosts and connected by communication subnet. The hosts are owned by the customer, whereas the communication subnet is typically owned and operated by a telephone company or Internet service provider. Subnet carries messages from host to host.
- A WAN is a geographically dispersed collection of LANs. A wide area network is simply a LAN of LANs or Network of Networks.
- WAN are characterized by the slowest data communication rates and the largest distances.
- Wide Area Networks are commonly connected either through the Internet or special arrangements made with phone companies or other service providers.
- WAN may use advanced technologies like Asynchronous Transfer Mode (ATM), Frame Relay and SONET.
- Internet, Indian Railway Reservation System, Bank Networks that supported core banking, etc. are some good examples of WAN. The Internet is the largest WAN, spanning the World today. Fig. 1.20 shows a typical WAN.

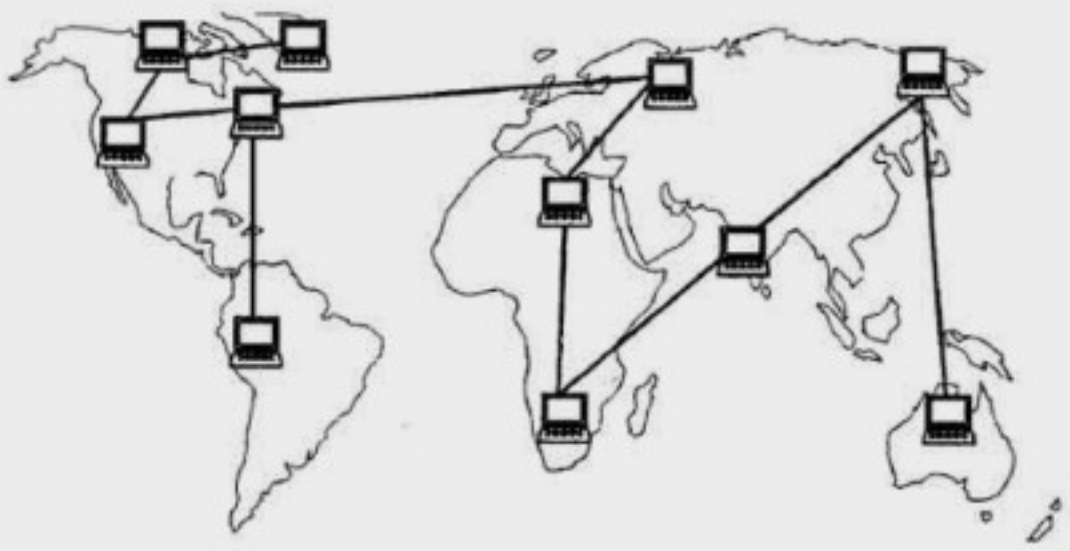


Fig. 1.20: WAN

- WAN contains a collection of machines used for running user (i.e. application) programs. All the machines called hosts are connected by a communication subnet.

- Fig. 1.21 shows communication Subnet and Host is WAN.

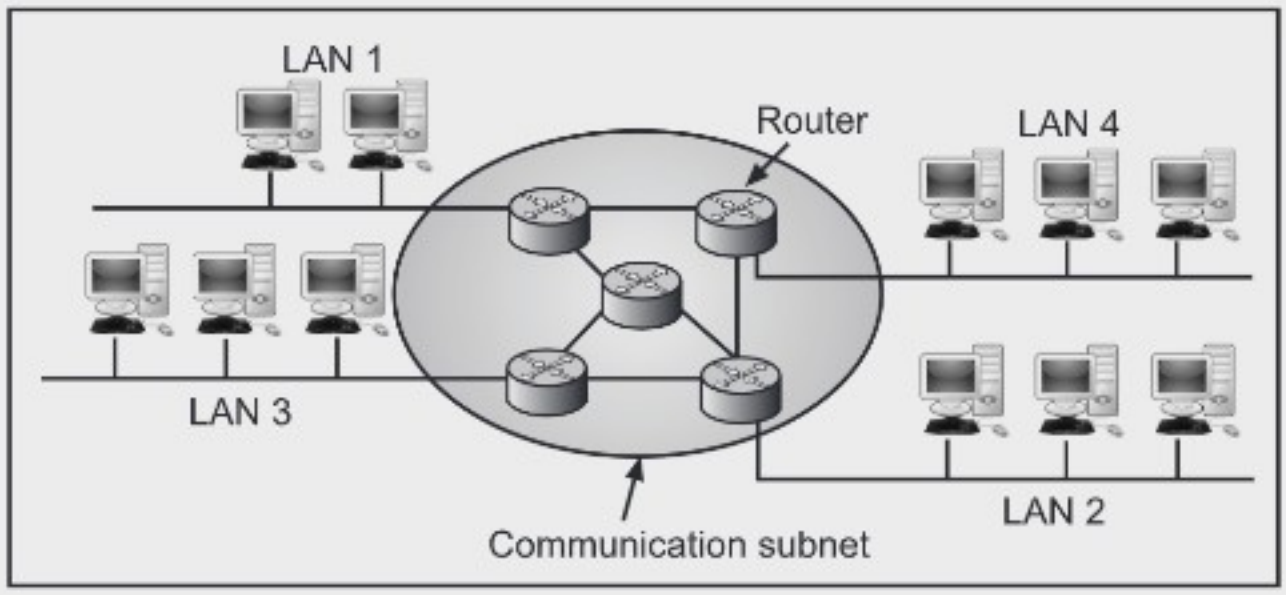


Fig. 1.21 Communication Subnet and Host is WAN

- The function of the subnet is to carry messages from host to host. The subnet consists of two important components; transmission lines and switching elements.
- Transmission lines move bits from one machine to another. The switching elements are specialized computers used to connect two or more transmission lines. When data arrive on an incoming line, the switching element must choose an outgoing line to forward them.
- The switching elements are either called as packet switching nodes, intermediate systems, data switching exchanges or routers.
- When a packet is sent from one router to another via one or more intermediate routers, the packet is received at intermediate router. It is stored in the routers until the required output line is free and then forwarded. A subnet using this principle is called a point to point, store-forward or packet switched subnet.
- WAN's may use public, leased or private communication devices, and can spread over a wide geographical area. A WAN that is wholly owned and used by a single company is often called as an enterprise network.

Advantages of WAN:

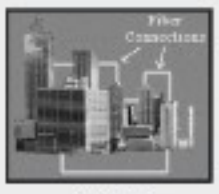
1. WAN covers a large geographical area.
2. WAN shares software and resources with connecting workstations.
3. Using WAN messages can be sent very quickly to anyone else on the network.
4. Expensive things (like printers or phone lines to the internet etc.) can be shared by all the computers on the network.
5. WAN adds fluidity to users information communication.

Disadvantages of WAN:

1. WANs are expensive.

2. Slow in speed than LAN and MAN.
3. WANs need a good firewall to restrict outsiders from entering and disrupting the network.
4. Setting up a network can be time consuming.
5. Protection against hackers and viruses adds more complexity and expense.

Table 1.3: Difference between LAN, MAN and WAN

Parameters	LAN	WAN	MAN
1. Stand for	Local Area Network.	Wide Area Network.	Metropolitan Area Network.
2. Area covered	Covers small area i.e. within the building (less than 1 km).	Covers large geographical area, like country, state etc.	Covers larger area than LAN and smaller than WAN like city, campus.
3. Error rates	Lowest.	Highest.	Moderate.
4. Transmission speed	High.	Low.	Moderate .
5. Equipment cost	Uses inexpensive equipment.	Uses most expensive equipment.	Uses moderately expensive equipment.
6. Example	Offices, Cyber Café.	Internet.	ATM, FDDI etc.
7. Data transfer rate	High.	Low.	Moderate.
8. Setup cost	Low.	High.	Moderate.
9. Diagram	 LAN	 WAN	 MAN

1.8.4 PAN

- A Personal Area Network (PAN) is a computer network organized around an individual person, and that's setup for personal use only.
- A PAN is a computer network used for data transmission amongst devices such as smartphones, tablets and Personal Digital Assistants (PDAs).
- In PAN devices are communicate over the range of a person. It can be wired or wireless.
- In wired PAN, devices like mouse, keyboard, and monitor are connected to the personal computer through cable.

- In wireless PAN, for a short range, Bluetooth is used for connecting components.
- Fig. 1.22 shows a user transferring data from a personal digital assistant via a personal area network to a workstation attached to a local area network.

Fig. 1.22 Personal Area Network(PAN)

Advantages:

1. PAN is portable type of network i.e., if a person moving from one place he can carry his portable devices such as laptops, mobile phones, PDAs and so on.
2. PANs are efficient, cost-effective and convenient.
3. PAN is secured because it is control by single person.

Disadvantages:

2. Shorter distance up to 10 meter only.
3. Data transfer rate is low compare to other networks.

1.8.5 Wireless Networks

- Wireless communication is one of the fastest growing technologies. The demand for connecting devices without the use of cables is increasing everywhere.
- The word wireless is dictionary defined as "having no wires".
- In networking terminology, wireless is the term used to describe any computer network where there is no physical wired connection between sender and receiver, but rather the network is connected by radio waves and/or microwaves to maintain communications.
- The basis of wireless systems is radio waves, an implementation that takes place at the physical level of network structure.
- Wireless networks can be divided into three main categories as System Interconnection, Wireless LANs, and Wireless WANs.

1. **System Interconnection:**

- System interconnection means connecting the components of computer using short range radio.
- All components can also be connected by a short range wireless network called Bluetooth. Bluetooth also allows digital cameras, headsets, scanners and other devices to connect to a computer.

- The system interconnection networks use the master-slave paradigm as shown in Fig. 1.23.

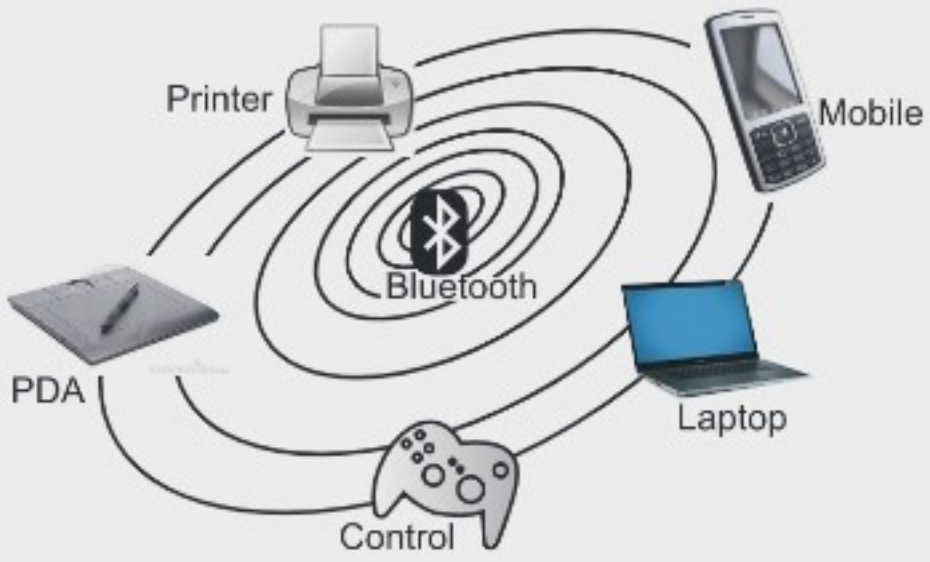
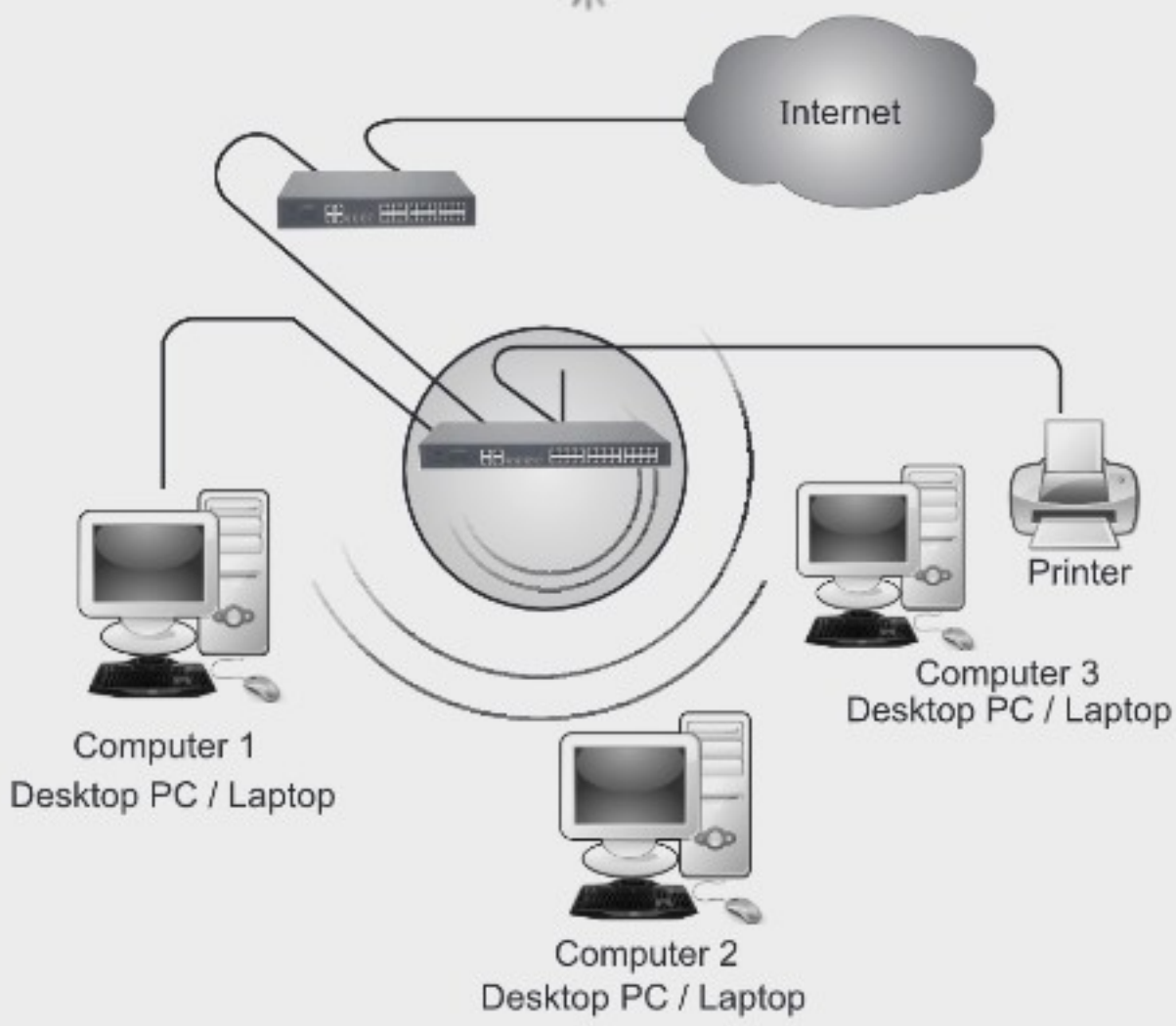


Fig. 1.23: Bluetooth Configuration

2. Wireless LANs:

- The next step in wireless networking are the wireless LANs. WLANs are systems in which every computer has a radio modem and antenna with which it can communicate with other system.
- Wireless LANs are becoming increasingly common in small offices and homes.
- IEEE 802.11 is a standard for wireless LANs.



- A Wireless Local Area Network (WLAN) links two or more devices over a short distance using a wireless distribution method, usually providing a connection through an access point for Internet access.

3. **Wireless WANs:**

- The third kind of wireless network is used in wide area system.
- The radio network used for cellular telephones is an example of a low-bandwidth wireless system.
- Cellular wireless networks are like wireless LANs, except that the distances involved are much greater and the bit rates are much lower.
- In addition to low-speed networks, high bandwidth wide area wireless networks are also being developed. The initial use is high speed wireless internet access from homes and business bypassing the telephone system.
- Wireless Wide Area Networks (WWANs) are wireless networks that typically cover large areas, such as between neighboring towns and cities, or city and suburb. These networks can be used to connect branch offices of business or as a public internet access system.

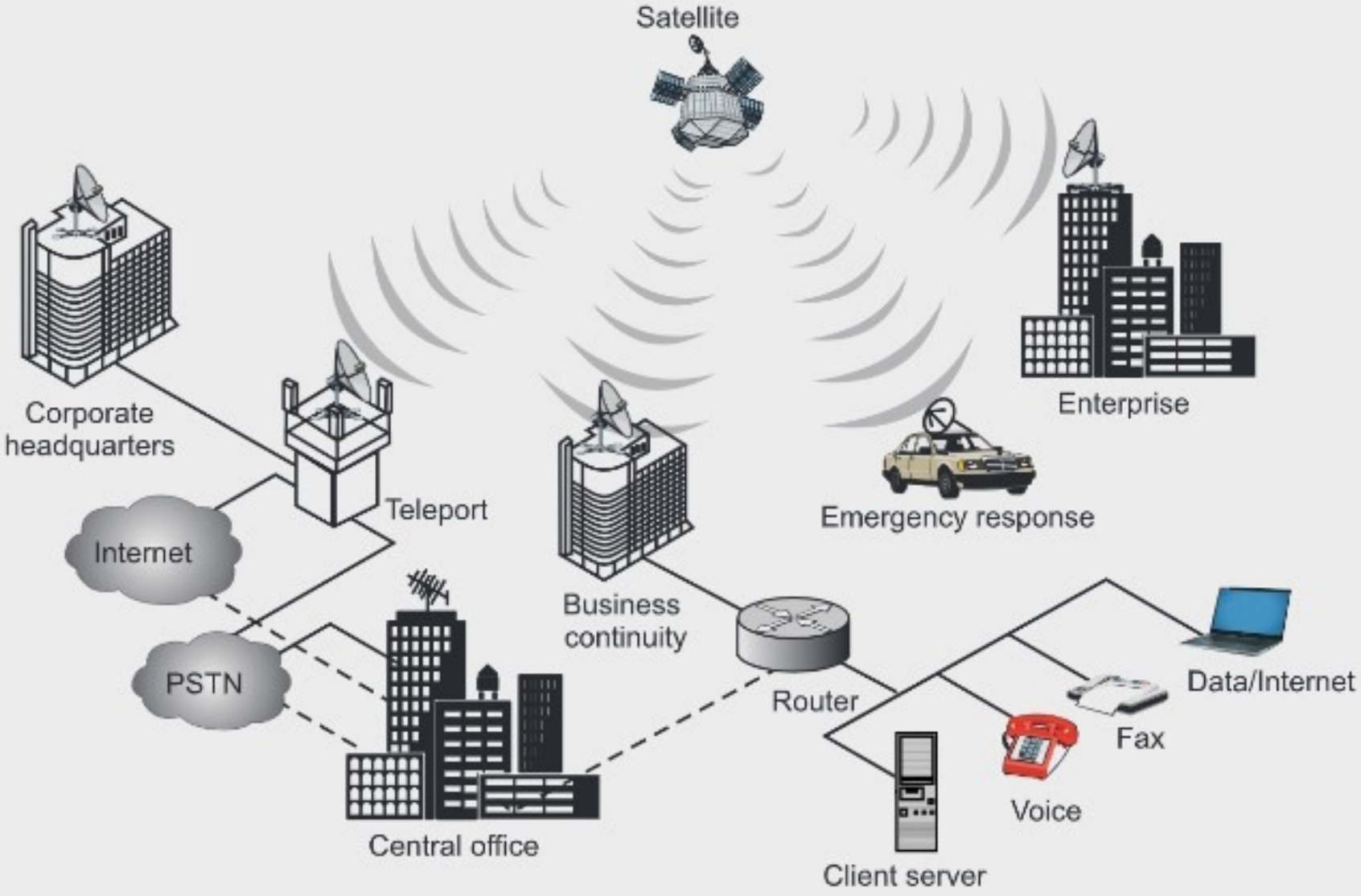


Fig. 1.25: WWAN

1.8.6 Home Networks

- The fundamental idea behind home networks is that in the future most homes will be setup for networking. Every device in the home will be capable of communicating with every other device and all of them will be accessible over the Internet.
- For example, with a PDA or mobile phone, a user can communicate with his microwave, refrigerator or babycam even though he/she is not at home.
- A Home Area Network (HAN) is a network that is deployed and operated within a small boundary, typically a House or Small Office/Home Office (SOHO).
- It enables the communication and sharing of resources (like the Internet) between computers, mobile and other devices over a network connection.
- A HAN is a dedicated network connecting devices in the home such as:
  1. Computers (PC, notebook, PDA etc.)
  2. Entertainment (TV, DVD, VCR, Camera, MP3 etc.)
  3. Telecommunications (telephone, mobile phone, fax, etc.)
  4. Appliances (microwave, refrigerator, lights, etc.)
  5. Telemetry (smoke alarm, babycam etc.)
- Home computer networking is already in a limited use, but more and more demands from users are there. Music and movies can be downloaded from the Internet, but now user want to connect stereos and television to it. People want to share their own videos with friend and family. Many parents want to monitor their babies on their PDA, mobile phone when they are at work.

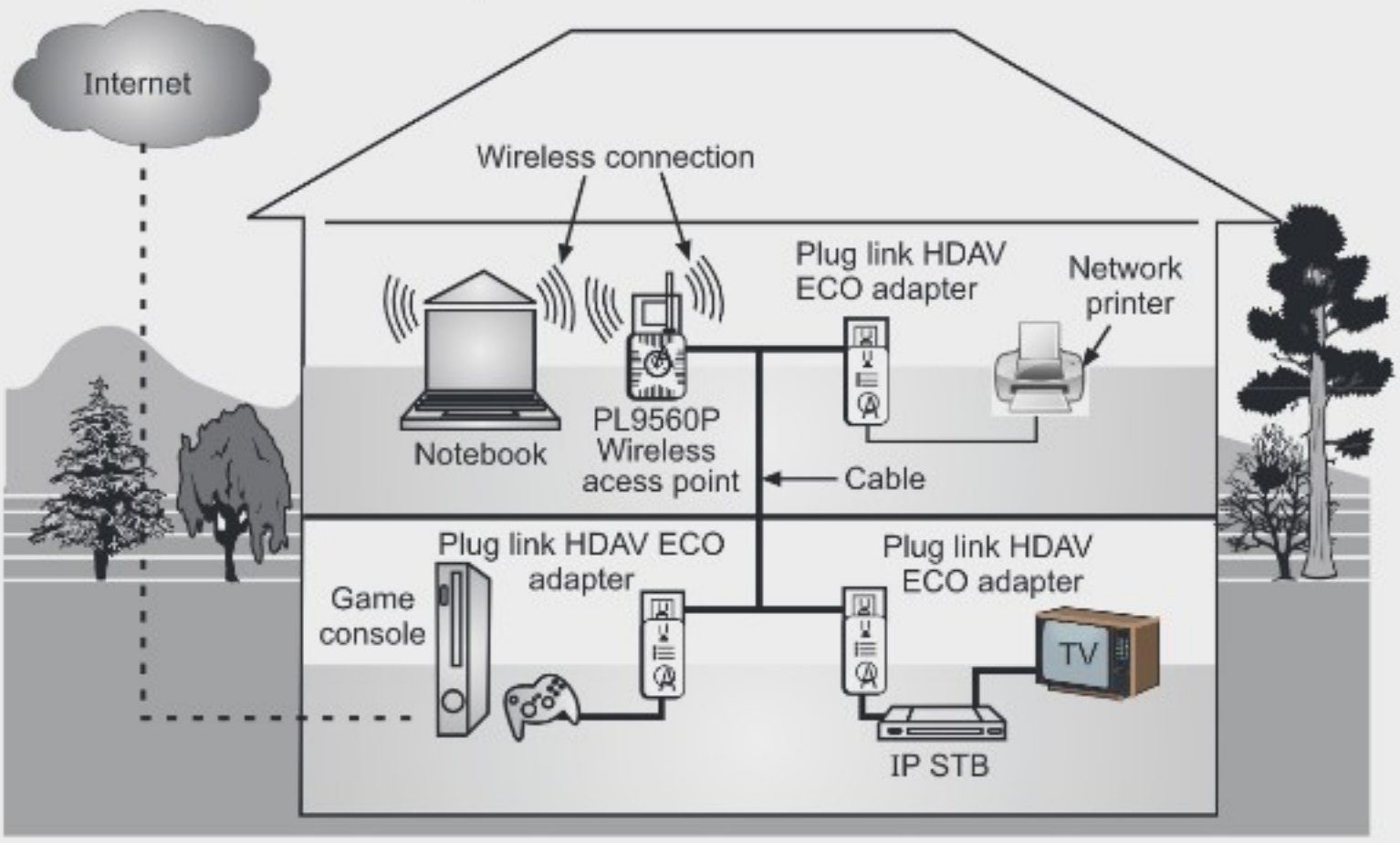


Fig. 1.26: Home Area Network (HAN)

- As a type of IP-based Local Area Network (LAN), a HAN may be wired or wireless. In a typical implementation, a HAN consists of a broadband Internet connection that is shared between multiple users through a vendor/third party wired or wireless modem. Fig. 1.26 shows a HAN.

Advantages:

1. The main advantage of a network is that multiple users can simultaneously interact with each other and share resources for example, the Internet connection.
2. After the home network is created, as many wireless devices like laptops and mobile phones can connect to it and more PC's can also be connected with ease and simple.

Disadvantages:

1. The equipments are so costly for buying.
2. Complete set up of a network can be difficult.
3. Depending on the network topology type, a broken cable can halt the whole network.

1.8.7 Internetworks or Internet

- Today, it is very rare to see a LAN, a MAN in isolation, they are connected to one another. When two or more networks are connected, they become an Internetwork or Internet.
- An internetwork is formed when distinct networks are interconnected. The Internet is a structured organized system.
- Internetworking started as a way to connect disparate types of computer networking technology.
- Computer network term is used to describe two or more computers that are linked to each other. When two or more computer networks or computer network segments are connected using devices such as a router then it is called as computer internetworking.
- Internetworking is a term used by Cisco. Any interconnection among or between public, private, commercial, industrial, or governmental computer networks may also be defined as an internetwork or Internetworking.
- An internetwork is a collection of individual networks, connected by intermediate networking devices, that functions as a single large network.
- Internetworking refers to the industry, products, and procedures that meet the challenge of creating and administering internetworks.
- The Internet has come a long way since the 1960s. The Internet today is not a simple hierarchical structure. It is made-up of many wide and local area networks joined by connecting devices and switching stations.

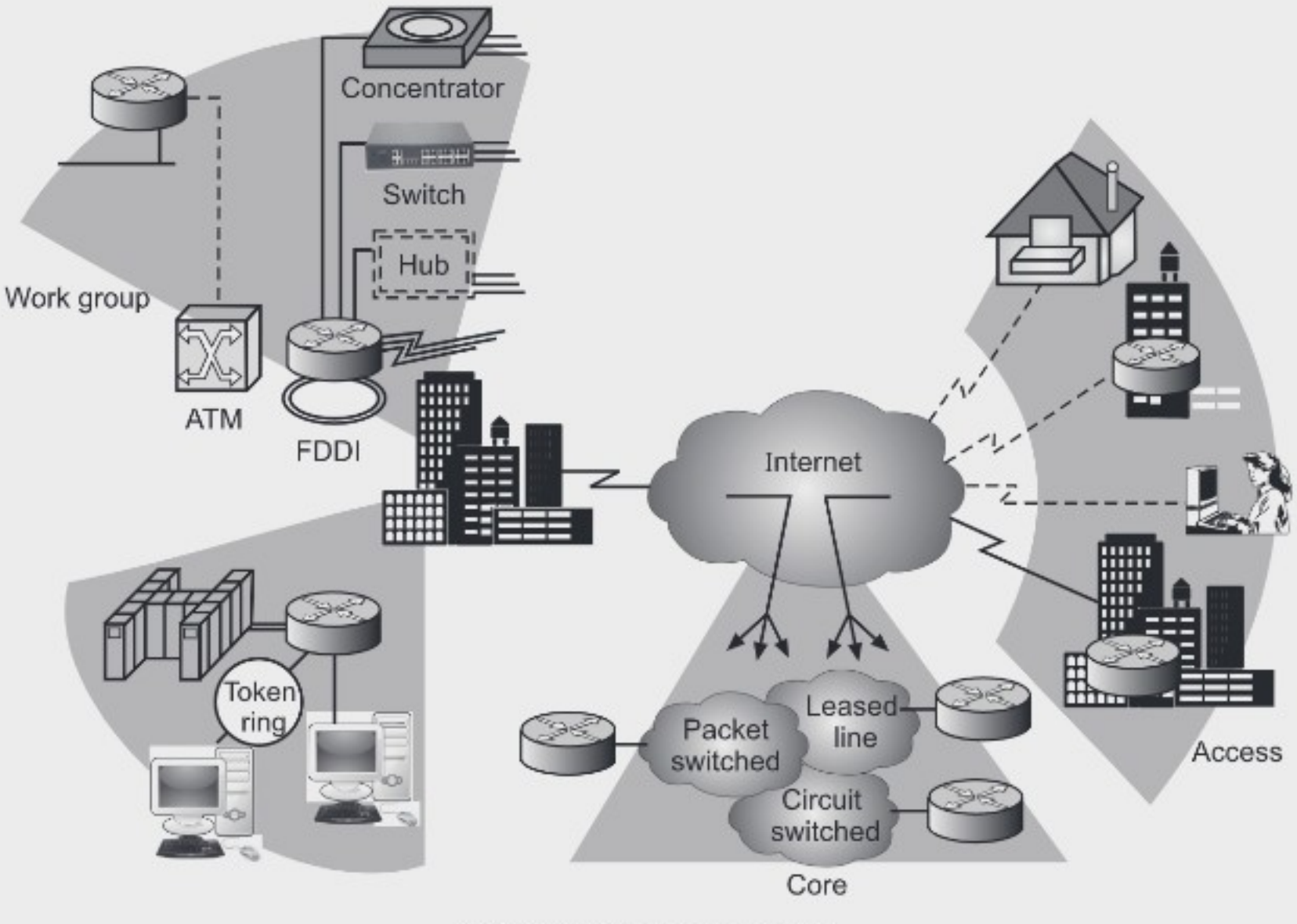


Fig. 1.27: Internetworking

- Today, most end users who want Internet connection use the services of Internet Service Providers (ISPs). There are international, national, regional and local service providers.
- There are following variants of Internetwork or Internetworking:
  1. **Intranet:** An intranet is a set of interconnected networks or Internetworking, using the Internet Protocol and uses IP-based tools such as web browsers and ftp tools, that is under the control of a single administrative entity.
  2. **Extranet:** An extranet is a network of internetwork or Internetworking, that is limited in scope to a single organization or entity but which also has limited connections to the networks of one or more other usually, but not necessarily, trusted organizations or entities.
  3. **Internet:** It is a network of networks based on many underlying hardware technologies, but unified by an internetworking protocol standard, the Internet Protocol Suite, often also referred to as TCP/IP.

Benefits of Internetworking:

1. Internetworks reduces network traffic.
2. The benefit of reduced traffic is optimized performance.

3. Network problems can be more easily identified and isolated in smaller networks, as opposed to one large network.
4. We can more efficiently span long distance by connecting multiple smaller networks.

1.9 PROTOCOLS AND STANDARDS – DEFINITION OF PROTOCOL, DEFACTO AND DEJURE STANDARD

- In this section, we will study two widely used terms: protocols and standards. The protocol, which is synonymous with rule and standards are agreed-upon rules. Without protocols and standards we wouldn't be able to achieve interoperability.

1.9.1 Protocols

- In computer networks, communication occurs between entities in different systems. An entity means sender and receiver that are capable of sending or receiving information. However, these entities cannot simply send bit streams to each other but expected to understand data bit streams. For communication to occur, the entities must agree on a protocol.
- For example, a printer needs to send messages to a computer telling it that it has run out of paper or that it is ready to print while a computer needs to send the data it wants to print to the printer.
- When two devices want to successfully communicate, they must agree to follows some rules about the way they will do it. These are known as protocols.

Definition of Protocol:

- A protocol is a set of rules that govern data communications which defines what is communicated, how it is communicated, and when it is communicated. It is an agreement between the communicating parties on how communication is to proceed.
- Violating the protocol will make communication more difficult, in fact impossible. Protocols may be implemented by hardware, software, or a combination of both.
- The key elements of a protocol are syntax, semantics, and timing.

Syntax:

- Syntax refers to the structure or format of data and signal levels. It indicates how to read the data in the form of bits or fields. It also decides the order in which the data is presented to the receiver.

Semantics:

- Semantics refers to the interpretation or meaning of each section of bits or fields. It specifies which field defines what action. It defines how a particular section of bits or pattern can be interpreted, and what action needs to be taken.

Timing:

- The term timing depicts two characteristics: when data should be sent and how fast they can be sent. A sender can send the data at a speed of 100 Mbps, but the receiver can consume it only at a speed of 20 Mbps, then there may be data losses or the packets might get dropped. So, proper synchronization must be there between a sender and a receiver.

1.9.2 Protocols Standards

- Standards are essential in creating and maintaining an open and competitive market for equipment manufacturers and in guaranteeing national and international interoperability of data and Telecommunications technology and processes.
- Standards provide guidelines to manufacturers, vendors, government agencies, and other service providers to ensure the kind of interconnectivity necessary in today's marketplace and in international communications.
- Standards are guidelines, these are more abstract. You can have products that meet the standard, exceed the standard or below a certain standard.
- Setting standards, rules that all manufacturers of hardware and software will follows, are important for a number of reasons:
- Standards describe accurately and unambiguously how information is transmitted.
- A manufacturer's products will work successfully with other manufacturer's products if they all follows the same standards.
- By defining a set of standards, you are providing a framework within which all manufacturers can design new, successful products.
- Standards break down complex ideas into smaller, methodical, easier to understand components.
- Data communication standards fall into two categories: De facto (i.e., meaning "by fact" or "by convention") and De jure (meaning "by law" or "by regulation").

De facto:

- The standards that have not been approved by an organized body but have been adopted as standards through widespread use are de facto standards. De facto standards are often established originally by manufactures who seek to define the functionality of a new product of technology.
- For example, The most important de facto organization involved in establishing communication standards and protocols is CCITT (Consultative Committee for International Telegraph and Telephone) is United Nations agency responsible for defining standards for Telegraph and Telephone. X.25 is most common standard for WAN.

- IBM (International Business Machines): SNA (System Network Architecture) protocol is example of De facto protocol. The IBM developed this protocol in 1974 for its mainframe computers, still being used by large number of organizations all over the world.

De jure:

- The De jure standards are have been legislated by an officially recognized body are de jure standards. A de jure standard is one developed and approved by an official organization.
- For example the IEEE (Institute of Electrical and Electronic Engineers) has the authority to create electrical standards such as wireless communication.
- On a global level ISO, the International Standards Organization was setup to create standards. They have produced over 18,500 formal standards covering everything from quality control to making tractors.

Summary

- Data communication refers to the exchange of data/information between two devices through some form of wired transmission medium (like coaxial cable, optic fiber cable etc.) or wireless transmission medium (like radio waves, micro waves, satellite communication and so on).
- Data communication is a process of exchanging data or information between two devices over a transmission medium.
- Computer network is a set or collection of computing devices that are linked to each other in order to communicate and share their resources with each other.
- The interconnected computers can share resources, which called networking.
- group of computers and other computing devices like printer connected together is called a network.
- Computer network is divided in to wired and wireless network. A wired network is simply a collection of two or more computers, printers, and other computing devices linked by cables like Ethernet, co-axial etc. cables. A wireless network, which uses high-frequency radio waves or micro wave rather than wires to communicate between nodes.
- Nowadays, computer networks have become an essential part of industry, entertainment world, business as well as our daily lives. Some of the applications of computer network in different fields are: Business applications, Home applications and Mobile application.

- Remote access is the ability to get access to a computer or a network from a remote distance. For examples, Home users get access to the Internet through remote access to an Internet Service Provider (ISP).
- is the act of transferring information through verbal messages, the written word, or more subtle, non-verbal signals. In Person to person communication Email is used on a daily basis by millions of people all over the world.
- computers, such as notebook computers and personal digital assistants (PDAs), are one of the fastest-growing segments of the computer industry.
- Social networking in forums, bulleting boards, Facebook, Twitter, etc., where people can exchange messages, photos, materials and other information with like-minded individuals or representatives of organizations can bring offense to other users.
- The widespread introduction of networking has introduced a whole new world of social, ethical, and political problems.
- Transmission Technology refers how two devices are connected and how they are communicating.
- The transmission technology can be categorized broadly into two type's i.e. Point-to-point networks and Broadcast networks (multipoint)
- Communication between two directly interconnected devices is referred to as point-to-point communication.
- Point-to-point networks consists of many connections between individual pairs of computers or machines.
- Point-to-point transmission with one sender and one receiver is sometime called unicasting.
- The networks having multipoint configuration are called Broadcast Networks.
- Another way of categorizing computer networks is through the scale of the network like PAN, MAN, WAN, LAN etc.
- Area Network (PAN) is the interconnection of devices within the range of an individual person, typically within a range of 1 meter.
- Local Area Network (LAN) is a privately-owned networks covering a small geographic area (10 m to 1 km), like a home, office, building or group of buildings (For example: campus).
- Metropolitan Area Network (MAN) covers a larger geographical area than is a LAN (1 km to 10 km), ranging from several blocks of buildings to entire cities.
- Wide Area Networks (WAN) covers a large geographical area (100 km to 1000 km), often a country.

- A collection of interconnected networks is called an internetwork or internet. The Internet is a global network connecting millions of computers.
- Network topology defines the geographic arrangement of computer networking devices.
- Topology defines the physical (describes the placement of network nodes and the physical connections between them) or logical (the paths that messages take to get from one place on the network to another place) arrangement of links in a network.
- Network topology is defined as, "the physical interconnection between various elements on computer network, such as links and nodes".
- There are a number of different network topologies in networking like star, ring, mesh, tree, bus etc.
- In bus topology, all nodes are connected to a central cable which is called a bus. This bus is also called as a Trunk or sometimes it was also referred to as Backbone cable.
- The bus network topology is also known as a linear bus because the computers in such a network are linked together using a single cable called a trunk, or backbone.
- In ring topology, the computers in the network are connected in a circular fashion which form of a ring.
- In star topology all the cables run from the computers to a central location, where they are all connected by a device called a hub/switch.
- A network structure whose design contains more than one topology is said to be Hybrid Topology. Two common examples for hybrid network are star ring network and star bus network.
- Computer networks fall into three classes regarding the size, distance and the structure namely LAN (Local Area Network), MAN (Metropolitan Area Network), WAN (Wide Area Network),
- The word wireless is dictionary defined as "having no wires". The computer networks that are not connected by cables of any kind are called as Wireless networks.
- Wireless networks can be divided into three main categories system interconnection (connecting the components of computer using short range radio like Bluetooth.
- A Wireless Local Area Network (WLAN) links two or more devices over a short distance using a wireless distribution method, usually providing a connection through an access point for Internet access.
- Wireless wide area networks are wireless networks that typically cover large areas, such as between neighboring towns and cities, or city and suburb. These networks can be used to connect branch offices of business or as a public internet access system.

- A Home Area Network (HAN) is a network that is deployed and operated within a small boundary, typically a house or Small Office/Home Office (SOHO). It enables the communication and sharing of resources (like the Internet) between computers, mobile and other devices over a network connection.
- An internetwork is a collection of individual networks, connected by intermediate networking devices, that functions as a single large network.
- Any interconnection among or between public, private, commercial, industrial, or governmental computer networks may also be defined as an internetwork or Internetworking.
- Any group of computers connected together can be called a data communications network, and the process of sharing resources between computers over a data communications network is called networking.
- A protocol is a set of rules that governs the communications between computers on a network.

Check Your Understanding

1. Which topology requires a central controller or hub?
   (a) Star (b) Mesh
   (c) Bus (d) Ring.
2. Which topology requires a multipoint connection?
   (a) Mesh (b) Star
   (c) Ring (d) Bus.
3. In a network with 25 computers, which topology would require the most extensive cabling?
   (a) Star (b) Mesh
   (c) Bus (d) Ring.
4. In a _____ connection, more than two devices can share a single link.
   (a) Point-to-point (b) Primary
   (c) Multipoint (d) Secondary.
5. _____ connection provides a dedicated link between two devices.
   (a) Multipoint (b) Point to Point
   (c) Primary (d) Secondary
6. In _____ transmission, the channel capacity is shared by both communicating devices at all times.
   (a) Simplex (b) Half duplex
   (c) Full Duplex (d) None of above

7. Communication between computer and keyboard involves a _____transmission.
   (a) Simplex (b) Half duplex
   (c) Full Duplex (d) None of above

ANSWER KEY

1. (a)	2. (d)	3. (b)	4. (c)	5. (b)
6. (c)	7. (a)			

Practice Questions

Q.1: Answers the Following Questions in short.

1. Mention different categories of computer networks (on the basis of scale).
2. What are the types of topologies?
3. What are the benefits of internetworking?
4. What are the two types of Transmission technologies, basis on which computer networks can be categorized?
5. List out components of data communication..

Q.2: Answers the Following Questions.

1. Define topology. Explain any one topology with its advantages and disadvantages.
2. Write a note on point-to-point and broadcast transmission.
3. What are the applications of computer networks ?
4. What is an internetwork ? Explain its structure in brief.
5. Write a short note on: (a) WAN, and (b) MAN.
6. Explain the layered network model. What are the advantages ?
7. Explain different types of LAN ? How do they differ in functionality ?
8. Describe home applications in detail.
9. Write short note on: (i) HAN (ii) Mobile users.
10. What are the different characteristics of data communication?
11. What are the goals of computer network?
12. What are the advantages and disadvantages of computer network.
13. Write about Protocol and Standards.
14. Explain types of data flows.

Q.3: Define the following terms.

(a) Topology
(b) Computer network

(c) Broadcasting
(d) Multicasting
(e) Internet
(f) Intranet
(g) Extranet

Previous Exams Questions

Summer 2019

1. Networking is a connection of two or more ..... . **[1 M]**

(i) Computer system
(ii) MAN
(iii) Place
(iv) WAN

2. Physical or logical arrangement of network is ..... . **[1 M]**

(i) Routing
(ii) Networking
(iii) Casting
(iv) Topology

3. Define Computer Network. **[1 M]**

Ans. Refer to section 1.5.1

4. What are important topologies for network ? **[1 M]**

Ans. Refer to section 1.7.1

5. Explain the characteristics on which data communication depends. **[4 M]**

Ans. Refer to section 1.2.1

6. Write a short note on Bus Topology. **[3 M]**

Ans. Refer to section 1.7.1.1

7. Write a note on WAN with its advantages and disadvantages. **[4 M]**

Ans. Refer to section 1.8.3

Winter 2018

1. In.....topology computer are connected in a circular fashion. **[1 M]**

(i) BUS
(ii) Star
(iii) Tree
(iv) Ring

2. HAN is..... **[1 M]**

(i) Hybrid area network

(ii) Home area network

(iii) Home access network

(iv) House access network

3. Which topology requires multipoint connection ? **[1 M]**

(i) Mesh

(ii) Star

(iii) Ring

(iv) Bus

4. List the different forms of data representations. **[1 M]**

Ans. Refer to section 1.3

5. State the goals of computer networks. **[5 M]**

Ans. Refer to section 1.5.2

6. Differentiate between point-to-point network and Broadcast network. **[3 M]**

Ans. Refer to section 1.6.2

7. Write a short note on Point-to-Point Network. **[4 M]**

Ans. Refer to section 1.6.1

Summer 2018

1. In a _____ connection, more than two devices can share a single link. **[1 M]**

(a) Point-to-point

(b) Primary

(c) Multipoint

(d) Secondary.

2. Define topology. **[1 M]**

Ans. Refer to section 1.7

3. Explain the characteristics on which data communication depends. **[4 M]**

Ans. Refer to section 1.2.1

4. Write short note on star topology. **[3 M]**

Ans. Refer to section 1.7.1.3

5. Give the advantages of computer network. **[4 M]**

Ans. Refer to section 1.5.4

❖❖❖

2...

Network Models

Objectives...

- To understand Concept of Network Models.
- To study OSI Reference Model.
- To learn TCP/IP Model and TCP/IP Protocol Suite.
- To learn Addressing used in TCP/IP Model.

2.1 INTRODUCTION

- In the 1st chapter, we discussed about network hardware and software. A network is a combination of hardware and software that sends data from one location to another.
- The hardware consists of the physical equipment that carries signals from one point to the network to another.
- The software consists of instruction sets, which make possible the services that we expect from a network.
- To solve any task with the help of a computer, we need the help of both hardware and software. We used the concept of layers in our daily life, for example, consider communication between two friends through postal mail.
- The process of sending a letter by one friend to another is difficult, if there are no services available by post office.
- In following Fig. 2.1, we have a sender, a receiver and a carrier
- At sender and receiver's end, all the activities done are grouped in three layers.
- The task of transporting the letter between the sender and receiver is done by the carrier. At the sender site, the letter must be written and dropped in the mailbox, before being picked up by the letter carrier and delivered to the post office.
- At the receiver site, the letter must be dropped in the recipient mailbox before being picked up and read by the recipient. Every step must be carried out sequentially one by one. In the same way computers also work.
- Each layer at sending site uses services of the layer immediately below it.

- Network models define a set of network layers and how they interact.

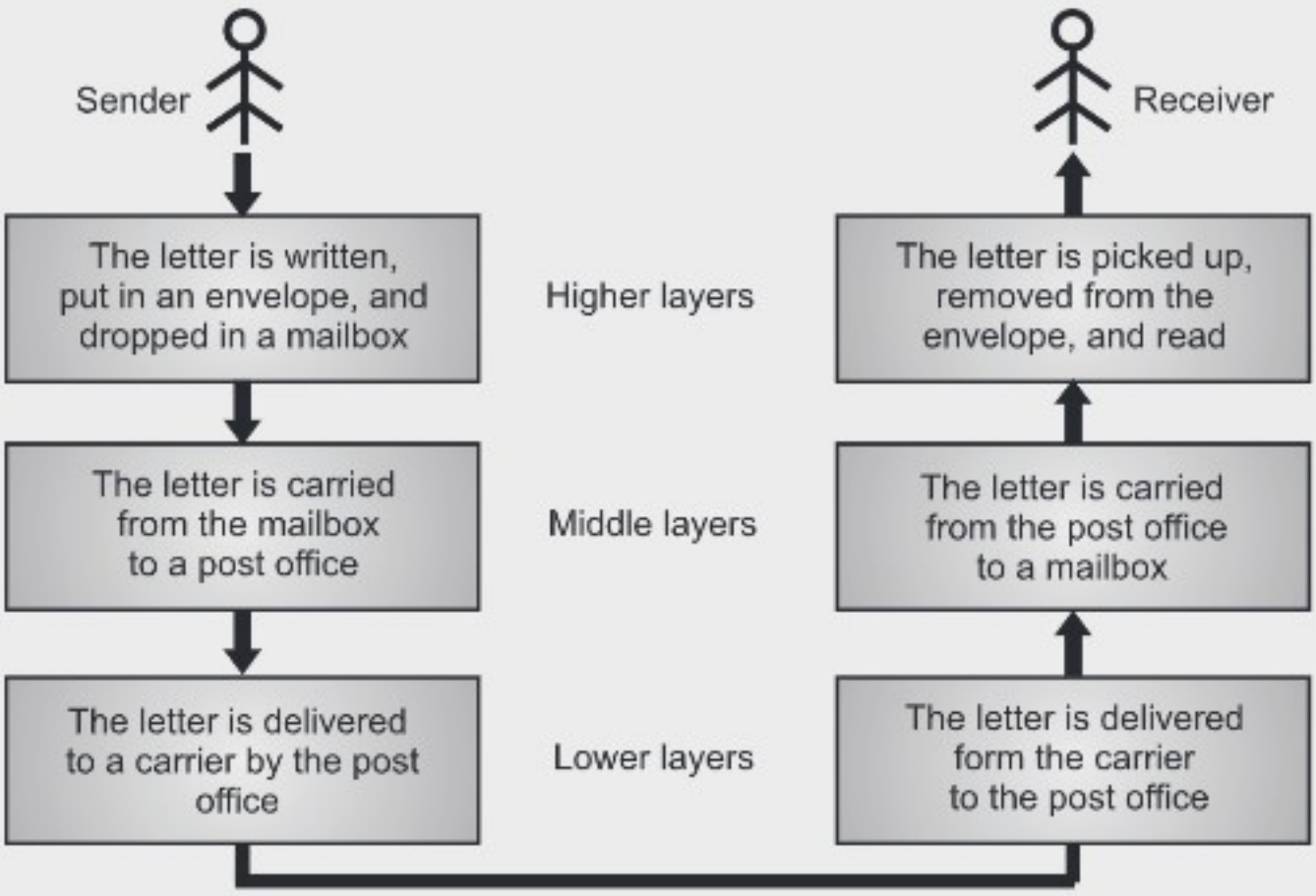


Fig. 2.1: Communication occurs between sender and receiver

- There are several different network models depending on what organization or company started them. The most important two models are:
  1. **OSI Network Model:** The International Standards Organization (ISO) has defined a standard called the Open Systems Interconnection (OSI) reference model. This is a seven layer architecture listed in the next section. This model dominated data communication and networking literature before 1990. The OSI model was never fully implemented.
  2. **TCP/IP Model:** It is also called the internet model because TCP/IP is the protocol used on the internet. The TCP/IP protocol suite became the dominant commercial architecture because it was used and tested extensively on the Internet.
- In the next two sections, we will discuss two important network architectures, the OSI reference model and the TCP/IP model, layers of these models and functions of each.

2.2 INTRODUCTION TO OSI REFERENCE MODEL (S-19, W-18)

- The OSI model was established in the 1970s by the International Standards Organization (ISO) which is a multinational body dedicated to worldwide agreement on international standards.
- The model is called the ISO 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.
- The OSI model has seven separate but related layers. The principles that were applied to arrive at the seven layers are:
  1. A layer should be created where a different level of abstraction is needed.
  2. Each layer should perform a well-defined function.
  3. The function of each layer must support internationally standardized protocols.
  4. The layer boundaries should be chosen to minimize the information flow across the interfaces.
  5. The number of layers should be sufficient one.
- Fig. 2.2 shows seven layers of OSI model.
- The OSI model allows complete interoperability between incompatible systems. Within a single machine, each layer calls upon the services of the layer just below it.
- For example, layer 4 uses the services of layer 3 and gives services to layer 5. Between machines, layer X on one machine communicates with layer X on another machine. This communication is governed by an agreed-upon series of rules and conventions called protocols. The processes on each machine that communicates at a given layer are called peer-to-peer processes.

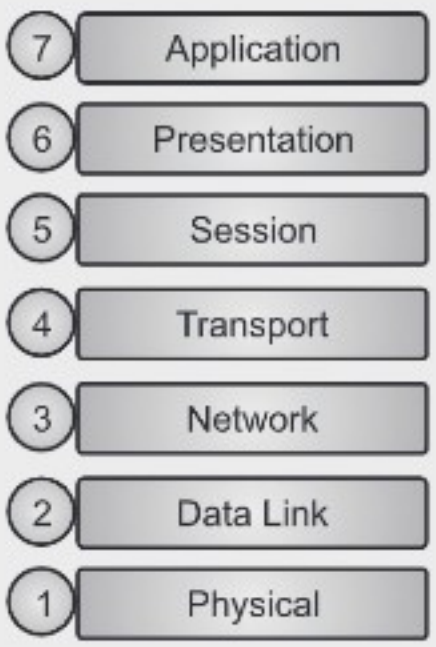


Fig. 2.2: OSI Reference Model

Basic Concepts in OSI Model:

Peer-to-Peer Processes:

- The entities comprising the corresponding layers on different computer machines are called peers.
- Within each machine, a layer calls upon the services of the layer below it while providing its own services to the layer above.
- At the physical layer, communication is direct i.e., Machine X sends a stream of bits to machine Y.

- At the higher layers, however, communication must move down through the layers on machine X, over to machine Y, and then back up through the layers.
- Each layer in the sending machine adds its own information to the message it receives from the layer just above it and passes the whole package to the layer just below it. This information is added in the form of headers or trailers (control data appended to the beginning or end of a data parcel).
- Headers are added to the message at layers 6, 5, 4, 3, and 2. X trailer is added at layer 2.
- Headers are added to the data at layers 6, 5, 4, 3, and 2. Trailers are usually added only at layer 2. At layer 1 the entire package is converted to a form that can be transferred to the receiving machine.
- At the receiving machine, the message is unwrapped layer by layer, with each process receiving and removing the data meant for it. For example, layer 2 removes the data meant for it, then passes the rest to layer 3. Layer 3 removes the data meant for it and passes the rest to layer 4, and so on.

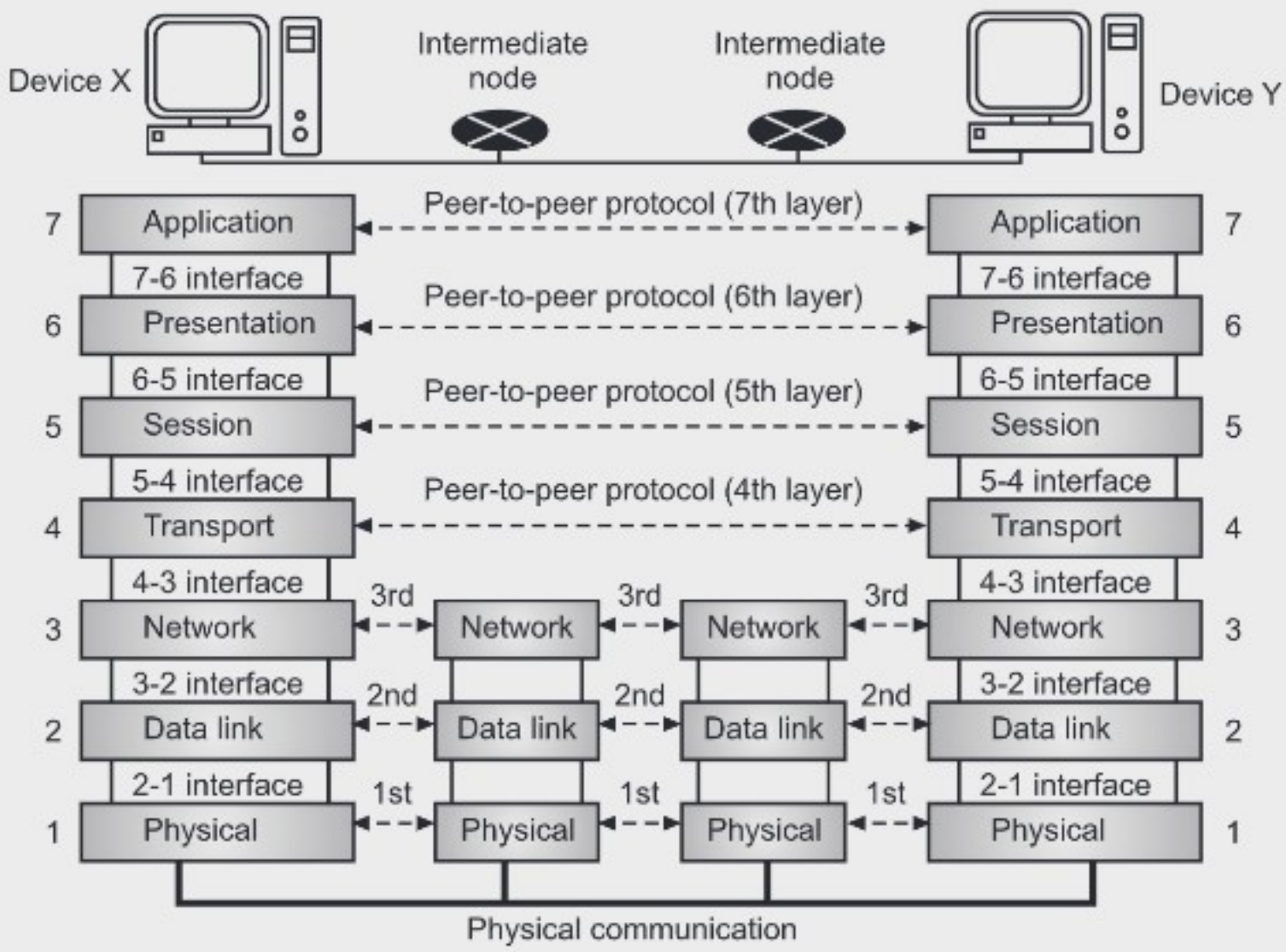


Fig. 2.3: Interactions between OSI Model Layers

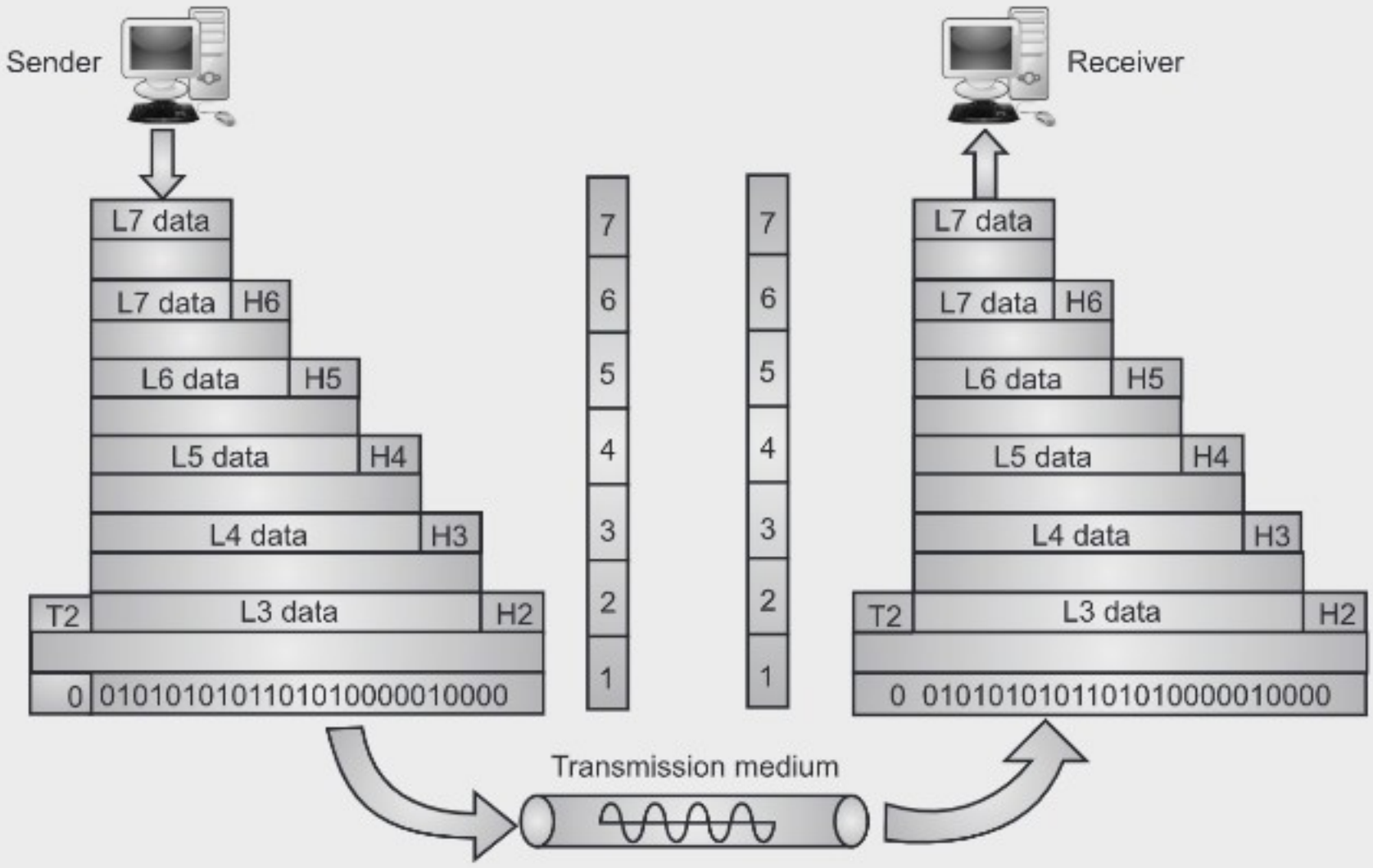


Fig. 2.4: An Exchange using OSI Model

Interfaces between Layers:

- The passing of the data and network information down through the layers of the sending machine and back up through the layers of the receiving machine is made possible by an interface between each pair of adjacent layers.
- Each interface defines what information and services a layer must provide for the layer above it.
- Well-defined interfaces and layer functions provide modularity to a network.

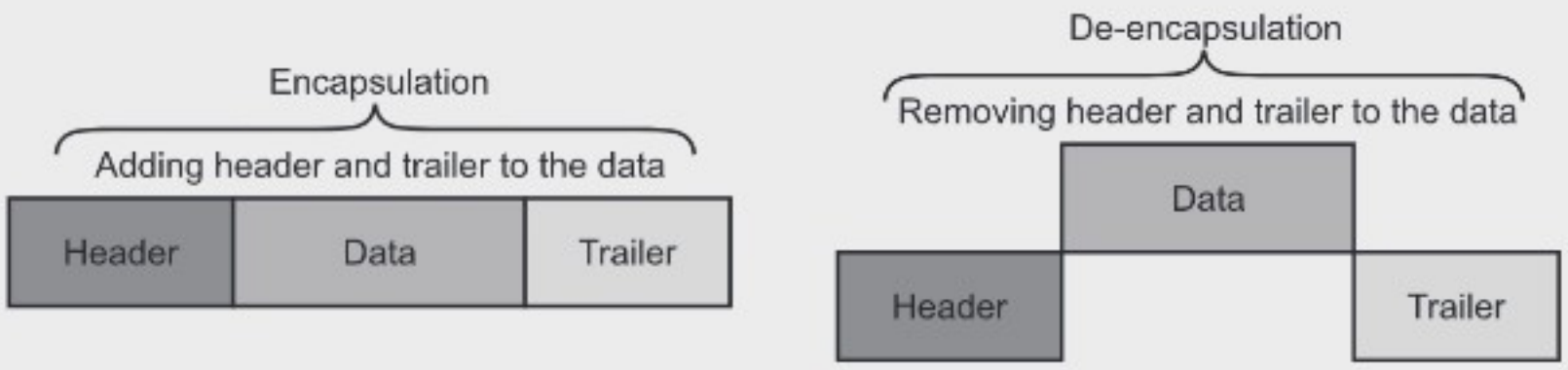
Organization of the Layers:

- All the seven layers are grouped into three subgroups. Layer 1, 2 and 3 are called network support layer and deal with the physical aspect of moving data from any device to another.
- Layer 5, 6 and 7 are called user support layers, and allows interoperability among unrelated software systems.
- Layer 4 links the two subgroups and ensures that what lower layers have transmitted is in a form that the upper layers can use.

Encapsulation:

- In networking models, the terms encapsulation and de-encapsulation refer to a process in which protocol information is added to the data and removed from the data when it passes through the layers.

- Protocol information can be added before and after the data. If information is added before the data, it is known as header. If information is added after the data, it is known as trailer.



(a): Encapsulation **(b): De-encapsulation**

Fig. 2.5

- Header and trailer added by a layer in the sending computer can be removed only by the peer layer in the receiving computer. For example, the header and trailer added by the transport layer in the sending computer can be removed only by the transport layer in the receiving computer.
- When data encapsulated by a layer of sending computer is processed by the same layer of receiving computer, it is known as the same layer interaction. Each layer adds its own header to the data supplied by the higher layer.
- Encapsulation takes place in the sending computer while the de-encapsulation process takes place in the receiving computer. After encapsulation, each layer uses a specific name or term to represent the encapsulated data. Following Table 2.1 shows that terms used by OSI model to represent encapsulated data.

Table 2.1: Lists the terms used by layers in OSI model to represent the encapsulated data

Term	OSI layer
Data	Application
Data	Presentation
Data	Session
Segment	Transport
Packet	Network
Frame	Data Link
Bits	Physical

2.2.1 Functions of Each Layer

- In this section, we will discuss the functions of each layer in the OSI model.

1. Physical Layer: **(W-18)**

- The physical layer is the lowest layer (1st) of the OSI model.
- The physical layer coordinates the functions required to carry a bit stream over a physical medium.
- Physical layer deals with the mechanical and electrical specifications of the interface and transmission medium.
- Physical layer also defines the procedures and functions that physical devices and interfaces have to perform for transmission to occur. The physical layer is responsible for movements of individual bits from one node to the next.
- The physical layer also concerned with the following functions:

(i) **Physical Characteristics of Interfaces and Medium:** Physical layer defines the characteristics of the interface between the devices and the transmission medium. It also defines the type of transmission medium.

(ii) **Representation of Bits (Data Encoding):** Below the physical layer there is a transmission medium, which carries computer data. Any transmission medium doesn't understand about computer data i.e. 0 and 1, it understands only about signals. Physical layer converts binary data into signals and vice versa. For this different type of encoding methods are used by the Physical layer.

(iii) **Data Rate:** Physical layer defines the transmission rate i.e. the number of bits sent in one second. Therefore it defines the duration of a bit.

(iv) **Bit Synchronization:** The sender and receiver must use the same bit rate as well as must be synchronized at the bit level. The sender and receiver clocks must be synchronized.

(v) **Line Configuration:** Physical layer also defines the way in which the devices are connected to the medium. Two different line configurations are used point to point configuration and multipoint configuration.

(vi) **Physical Topology:** The physical topology defines how devices are connected to form a network. Devices can be connected by using star, ring, mesh, bus etc. topologies.

(vii) **Transmission Mode:** Physical layer also defines the way in which the data flows between the two connected devices. The various transmission modes possible are simplex, half-duplex and full-duplex.

2. Data Link Layer:

- The 2nd layer of the OSI model is the Data link layer.

- The data link layer is responsible for moving frames from one node (hop) to the next. Data link layer transforms the physical layer, a raw transmission facility to a reliable link (error free) and gives it to the network layer.
- It is often divided into two parts:
  (i) **Media Access Control (MAC):** The MAC sub layer controls the means by which multiple devices share the same media channel. This includes contention methods and other media access details. The MAC layer also provides addressing information for communication between network devices.
  (ii) **Logical Link Control (LLC):** The LLC sub layer establishes and maintains links between communicating devices.
- Functions of data link layer are:
  (i) **Framing:** The data link layer divides the stream of bits received from the network layer to manageable data units called frames. Data link layer performs various framing functions like Frame Traffic Control, Frame Sequencing, Frame Delimiting and so on.
  (ii) **Physical Addressing:** The physical addresses have authority over the network only. If frames are to be distributed to different systems on the network, a data link layer adds physical addresses to the frame to define the sender and/or receiver. If the receiver is outside the network, the receiver address is the address of the device that connects the network to the next one.
  (iii) **Flow Control:** Flow control is the traffic regulatory mechanism implemented by Data Link layer that prevents the fast sender from drowning the slow receiver
  (iv) **Error Control:** It provides the mechanism of error control in which it detects and retransmits damaged or lost frames. Data link layer also deals with the problem of duplicate frames, thus providing reliability to the physical layer.
  (v) **Media Access Management:** Data link layer determines when the node "has the right" to use the physical medium.
  (vi) **Access Control:** When two or more devices are connected to the same link, data link layer protocols decides which device has control over the link at a given time. Means data link layer protocols decides which device is going to use the link (for transmission etc.) at what time.

3. Network Layer: **(W-18)**

- The 3rd layer of the OSI model is the network layer.
- The network layer is responsible for the delivery of individual packets from the source host to the destination host.
- When source and destination are from the same network, there is usually no need for network layer, delivery of packets is handled by data link layer. However, if source

and destination are from different networks, the network layer is responsible for delivery of data packets.

- Other functions of network layer are:

(i) **Logical Addressing:** In order to identify each device on internetwork uniquely, network layer defines a logical addressing scheme, which distinguishes each device uniquely and universally on the Internet. When source and destination are from different networks, to deliver the packet logical addresses (IP) are required.

(ii) **Routing:** To go from any source to any destination on the Internet multiple paths are available. Out of these multiple paths, one path has to be selected. The selection is depending on certain criteria, this criteria is called as routing protocols and the entire procedure is called as routing. The network layer protocols determine which route or path is best from source to destination.

(iii) **Congestion Control:** This layer is also responsible for handling the congestion problem at the node, when there are too many packets stored at the node to be forwarded to the next node.

(iv) **Internetworking:** One of the main responsibilities of a network layer is to provide internetworking between different networks. It provides a logical connection between different types of network.

4. Transport Layer:

- The 4^{th} layer of the OSI model is the transport layer.
- Transport layer is responsible for process the process delivery of the entire message. A process is an application program running on a host.
- Network layer is not able to recognize the relationship among the packets, though the packets are from one message only, it only performs source to destination delivery.
- It treats each packet independently. The transport layer on the other hand, ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source to destination.
- Other functions of transport layer are:

(i) **Service-point Addressing (Port Addressing):** The purpose of the transport layer is to deliver messages from one process running on source machine to another process running on destination machine. It may be possible that several programs or processes are running on both the machines at a time. In order to deliver the message to the correct process, the transport layer header includes a type of address called service point address or port address. Thus by specifying this address, the transport layer makes sure that the message is delivered to the correct process on the destination machine.

(ii) **Segmentation and Reassembly:** Transport layer accepts a message from the (session) layer above it, splits the message into smaller units (if not already small enough), and passes the smaller units down to the network layer. The transport layer at the destination station reassembles the message.

(iii) **Connection Control:** The transport layer can provide connection oriented or connectionless services for connection control. A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination. A connection oriented transport layer makes a connection with the destination transport layer first and then delivers data. After all data transfer is done the connection is terminated.

(iv) **Flow Control:** Like Data link layer, transport layer also performs flow control. Transport layer makes sure that the sender and receiver communicate at a rate they both can handle. Therefore flow control prevents the source from sending data packets faster than the destination can handle. Flow control performed by transport layer is end to end.

(v) **Error Control:** Like Data link layer, Transport layer also performs error control. Here error control is performed end-to-end rather than across a single link. Error correction is usually achieved through retransmission.

5. Session Layer:

- The 5^{th} layer of the OSI model is the session layer.
- Session layer has the primary responsibility of beginning, maintaining and ending the communication between two devices, which is called Session.
- It also provides for orderly communication between devices by regulating the flow of data.
- The session layer is the network dialog controller. It establishes, maintains and synchronizes the interaction among communicating systems.
- Other function of session layer are:

  (i) **Dialog Control:** Dialog control is the function of the session layer that determines which device will communicate first and the amount of data that will be sent. It also decides the communication between two processes to take place in either half duplex of full duplex mode.

  (ii) **Synchronization:** Session layer allows a process to add synchronization points or check points, to a stream of data. The session layer decides the order in which data need to be passed to the transport layer.

6. Presentation Layer:

- The 6th layer of the OSI model is the presentation layer.
- The Presentation Layer is also called as Translation layer. The presentation layer presents the data into a uniform format and masks the difference of data format between two dissimilar systems. The presentation layer is concerned with the syntax and semantics of the information transmitted between two systems. Presentation layer is responsible for translation, compression and encryption.
- Specific responsibilities/functions are:
  - **(i) Translation:** The translation between the sender and the receiver's message formats done by the presentation layer if the two formats are different.
  - **(ii) Encryption:** Converting computer data into non-readable form is encryption. It is required for important data transmission. Decryption reverses the original process to transform the message back to its original form.
  - **(iii) Compression:** Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such as text, audio and video.

7. Application Layer:

- The 7th layer of the OSI model is the application layer.
- The application layer enables the user (human or software), to access the network. It provides user interfaces and support for services such as e-mail, remote file access and transfer, shared database management and other types of distributed information services. Application layer is responsible for providing services to the user.
- Other functions of application layer are:
  - **(i) Network Virtual Terminal:** A network virtual terminal is a software version of a physical terminal and it allows a user to log onto a remote host. The remote host believes it is communicating with one of its own terminals and allows the user to log on.
  - **(ii) File Transfer, Access and Management:** This application allows a user to access files in a remote host, to retrieve files from a remote host for use in the local computer and to manage or control files in a remote computer locally.
  - **(iii) Mail Services:** This application provides e-mail operations like forwarding and storage.
  - **(iv) Directory Services:** This application provides distributed database sources and access for global information about various objects and services.

2.2.2 Summary of OSI Layers

- Following table gives summary of functions of each layer of OSI Model.

Table 2.2: Functions of each layer of OSI Model

OSI Layer	Major Functions
1. Physical Layer	1. Defines voltage/signal rates and the physical connection methods. 2. Defines the physical topology. 3. Defines the physical structure of the network.
2. Data link Layer	1. Defines the method by which the media is accessed. 2. Performs error detection and handling for the transmitted signals. 3. Defines hardware addressing through the MAC sublayer.
3. Network Layer	1. Provides mechanisms for the routing of data between devices across single or multiple network segments. 2. Handles the discovery of destination systems and addressing.
4. Transport Layer	1. Determines the ordering and priorities of data. 2. Establishes, maintains, and breaks connections between two devices.
5. Session Layer	1. Handles error detection and notification to the peer layer on the other device. 2. Synchronizes the data exchange between applications on separate devices.
1. Presentation Layer	1. Converts data from the application layer into a format that can be sent over the network. 2. Handles encryption and decryption of data. Provides compression and decompression functionality. 3. Converts data from the session layer into a format that can be understood by the application layer.
7. Application Layer	1. Displays incoming information and prepares outgoing information for network access. 2. Provide access to the network for applications and certain end user functions.

2.3 TCP/IP REFERENCE MODEL (W-18)

- The ARPANET, a research network, which was developed by the U.S. department of defense, connected with hundreds of universities and government installations using leased lines.
- When satellite and radio networks were added to these networks, compatibility issues arose. The existing protocols are not compatible with new networks. So, no communication in between old and new networks.
- A new architecture is needed which connects multiple networks in a seamless way.
- A flexible architecture was needed since applications with diverse requirements were envisioned, ranging from transferring files to real time speech transmission. This architecture was developed and known as TCP/IP reference model.
- TCP/IP stands for Transmission Control Protocol/Internet Protocol.
- TCP/IP model also called the Internet reference model.
- The TCP/IP is a set of protocols, or a protocol suite, that defines how all transmissions are exchanged across the Internet.
- Fig. 2.6 shows TCP/IP model.

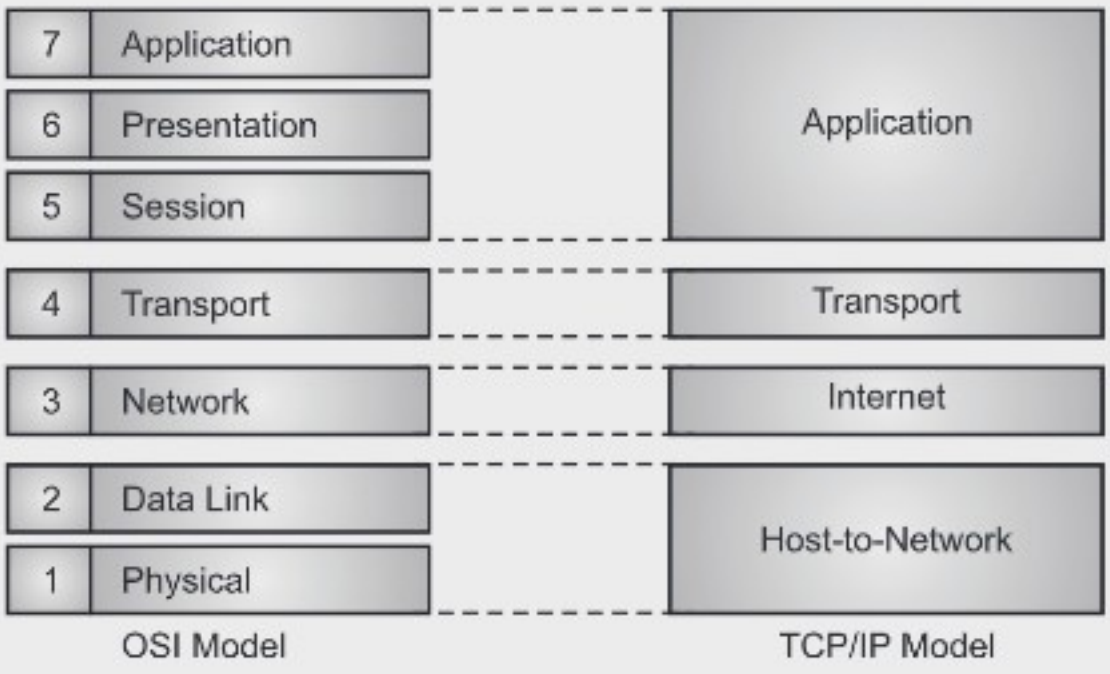


Fig. 2.6: TCP/IP Model

TCP/IP Model contains following Layers:

1. Host-to-Network Layer:

- Host-to-network layer is the first layer of the four layer TCP/IP model.
- This layer corresponds to the physical and data link layer of the OSI model.
- Host-to-network layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices

that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.

- The protocols included in the Host-to-network layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

2. Internet Layer:

- Internet Layer is the second layer of the four layer TCP/IP model.
- Internet layers pack data into data packets known as IP datagrams, which contain source and destination address (logical address or IP address) information that is used to forward the datagrams between hosts and across networks. The Internet layer is also responsible for routing of IP datagrams.
- Internet layer's job is to allow hosts to insert packets into any network and have them delivered independently to the destination.
- The main protocols included at Internet layer are IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol) and IGMP (Internet Group Management Protocol).

3. Transport Layer:

- Transport Layer is the third layer of the four layer TCP/IP model.
- The purpose of the Transport layer is to permit devices on the source and destination hosts to carry on a conversation.
- Transport layer defines the level of service and status of the connection used when transporting data.
- It is designed to allow peer entities on the source and destination hosts to carry on a conversation. We call it end-to-end communication.
- For this communication, two end-to-end protocols TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are used.

4. Application Layer:

- Application layer is the top most 4^{th} layer of the TCP/IP model.
- Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.
- Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol) , DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

2.4 TCP/IP PROTOCOL SUITE

- The TCP/IP protocol suite was developed prior to the OSI model. Therefore, the layers in the TCP/IP protocol suite do not exactly match those in the OSI model.
- The original TCP/IP protocol suite was defined as having four layers i.e. host-to-network, internet, transport, and application.
- However, when TCP/IP is compared to OSI, we can say that the host-to-network layer is equivalent to the combination of the physical and data link layers. The internet layer is equivalent to the network layer, and the application layer is roughly doing the job of the session, presentation, and application layers with the transport layer in TCP/IP taking care of part of the duties of the session layer. So in this section, we assume that the TCP/IP protocol suite is made of five layers: physical, data link, network, transport and application.
- The first four layers provide physical standards, network interfaces, internetworking and transport functions that correspond to the first four layers of the OSI model.
- The three topmost layers in the OSI model, however, are represented in TCP/IP by a single layer called the application layer as shown in Fig. 2.7.

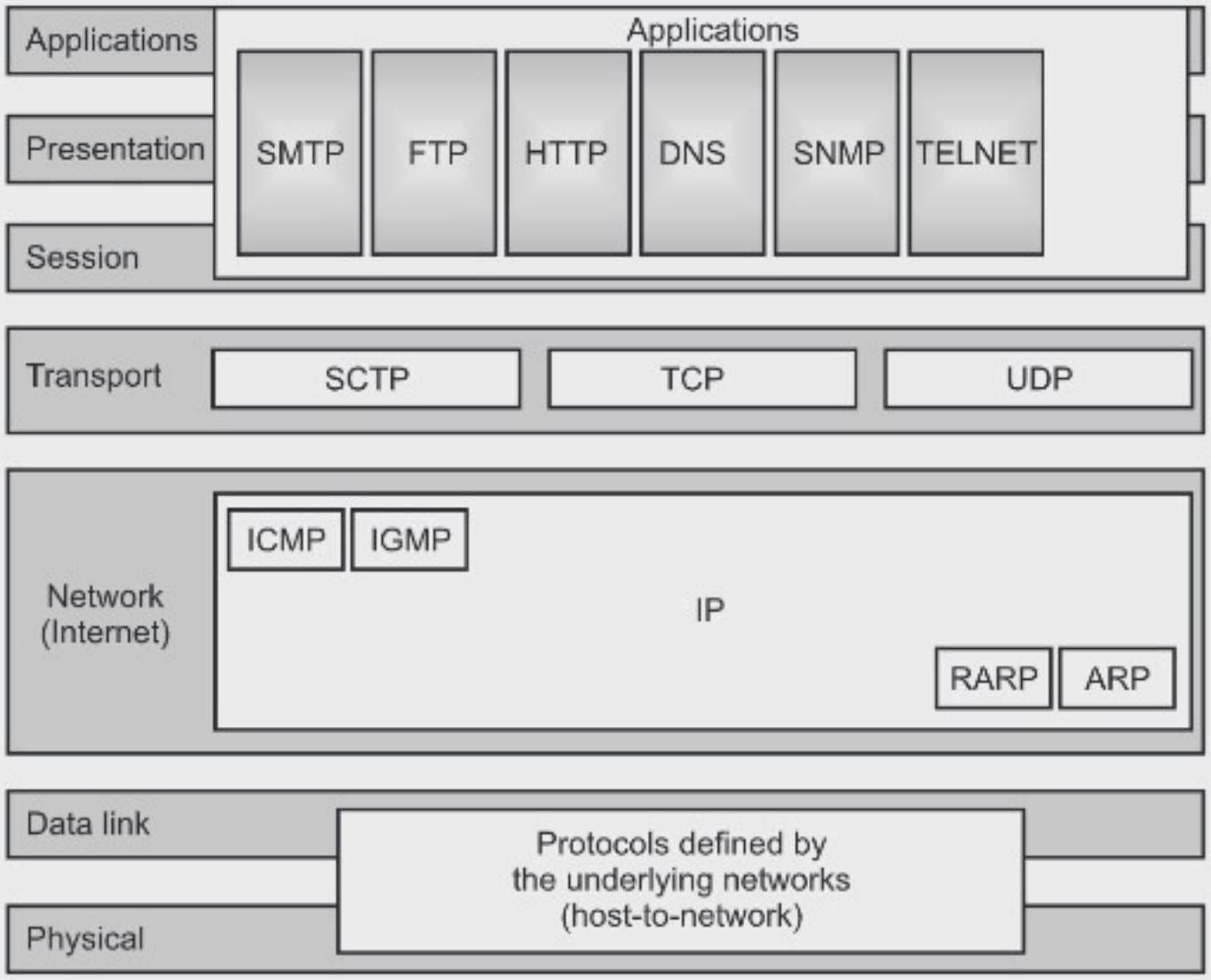


Fig. 2.7: TCP/IP and OSI Model

- TCP/IP is a hierarchical protocol made up of interactive modules with specific functionality. These modules are not interdependent. In the OSI model, every layer is having predefined functions. The layers in TCP/IP protocol suite contain relatively independent protocols that can be mixed and matched depending on the needs of the system. Every upper layer protocol is supported by one or more lower level protocols.

2.5 COMPARISON OF OSI AND TCP/IP MODELS (S-18, 19)

- The OSI and TCP/IP reference models have many things common. Both are based on concept of a stack of independent protocols.
- Functionality of the layers are almost the same. The layers above transport are application oriented users of the transport service.
- Despite these fundamental similarities, the two models also have many differences.
  1. First difference between these two is obviously the number of layers. OSI has seven layers whereas TCP/IP has four layers.
  2. The OSI model makes a clear distinction between services, interfaces and protocols, whereas TCP/IP model does not clearly distinguish between them.
  3. OSI model supports connection oriented and connectionless service in the Network layer and only connection oriented service in Transport layer. TCP/IP has connectionless service in Network layer but connection oriented and connectionless services in Transport layer.
  4. The protocols in the OSI model are hidden than in the TCP/IP model.
  5. The OSI reference model was developed before the corresponding protocols were invented. The model was not biased toward one particular set of protocol.
- Whereas, TCP/IP protocols were developed first, hence it does not fit into any other protocol stack.

2.6 ADDRESSING

- A network address is a unique identifier for a node of a computer network. Addressing is the mechanism for identifying senders and receivers on the computer network.
- TCP/IP protocol suite uses four different types of addresses as shown in Fig. 2.8.
  1. **Physical addresses (link):** Function of data link layer.
  2. **Logical addresses (IP):** Function of network layer.
  3. **Port addresses:** Function of transport layer.
  4. **Specific addresses:** Supported by application layer.

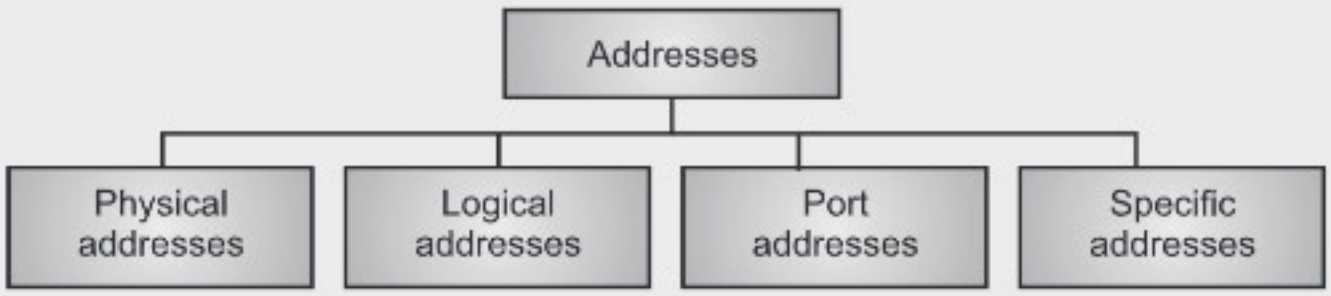


Fig. 2.8: Addresses in TCP/IP

- Each address is related to a specific layer in the TCP/IP architecture, as shown in Fig. 2.9.

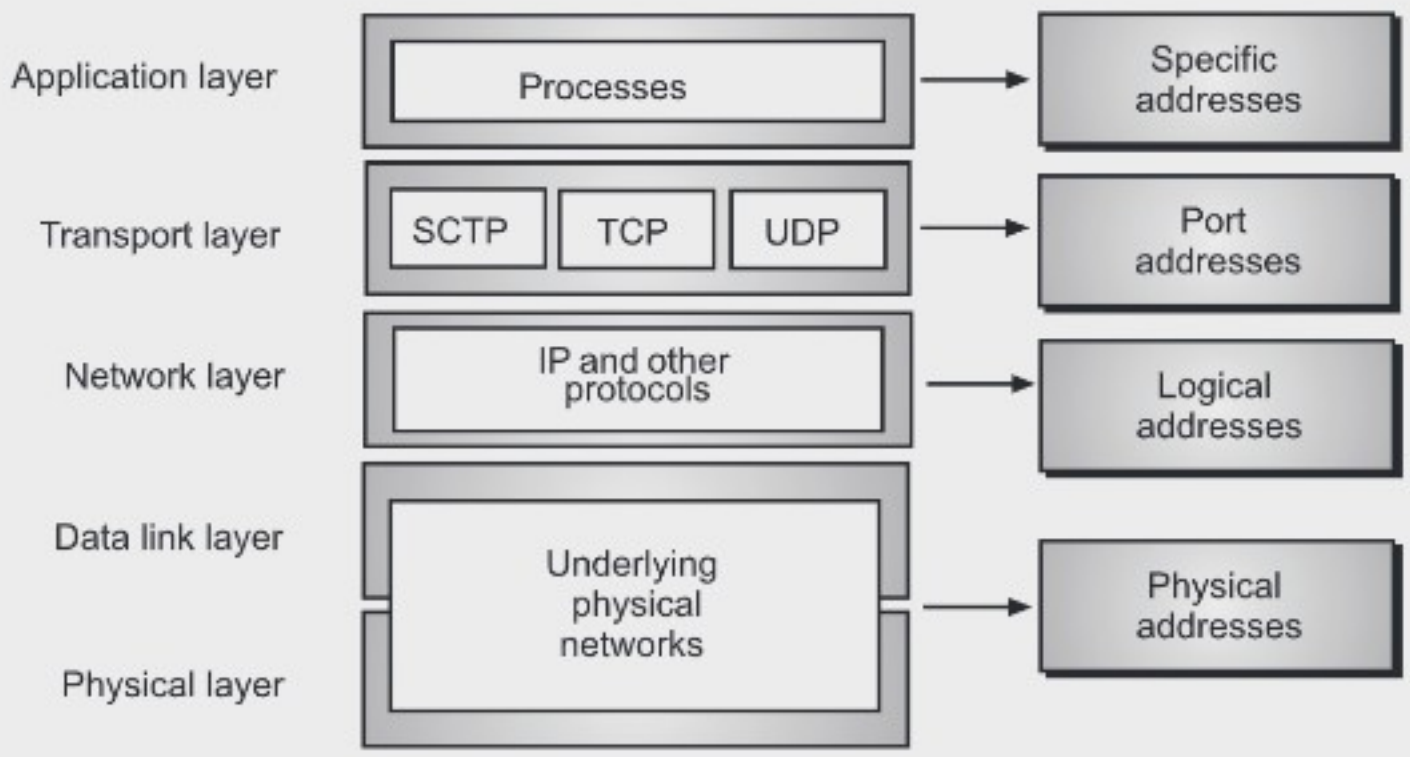


Fig. 2.9: Addresses related to each layer in TCP/IP architecture

1. **Physical Addresses:**

- The physical address also known as the link address, is the address of the node as defined by its LAN and WAN.
- Data link layer includes this address into the data frame.
- Physical address is used when source and destination are from the same network. It is the lowest level address.
- The physical addresses have authority over the network i.e. LAN or WAN. The address size and format depend on the network.
- For example, Ethernet uses 6 byte (48 bit) physical address which is imprinted on the network interface card (LAN card).

Example:

- In Fig. 2.10 a node with physical address 10 sends a frame to a node with physical address 87, The two nodes are connected by a link i.e., bus topology LAN.

- At the data link layer, this frame contains physical (link) addresses in the header. These are the only addresses needed. The rest of the header contains other information needed at this level. The trailer usually contains extra bits needed for error detection.
- Fig. 2.10 shows, the computer with physical address 10 is the sender, and the computer with physical address 87 is the receiver. The data link layer at the sender receives data from an upper layer. It encapsulates the data in a frame, adding a header and a trailer. The header, among other pieces of information, carries the receiver and the sender physical (link) addresses.

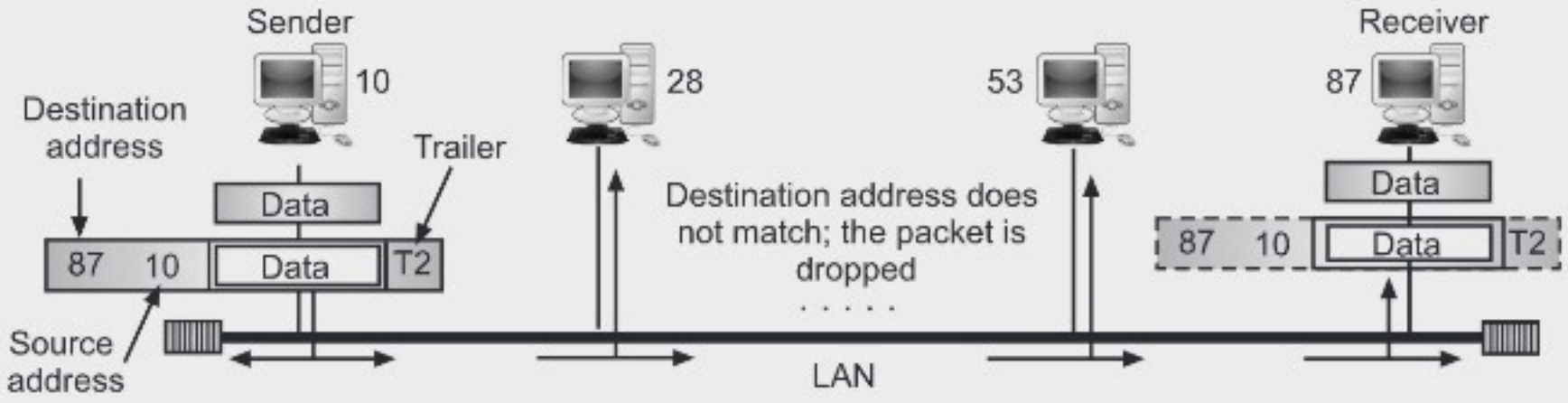


Fig. 2.10: Physical Addresses

- We have shown a bus topology for an isolated LAN. In a bus topology, the frame is propagated in both directions (left and right).
- The frame propagated to the left dies when it reaches the end of the cable if the cable end is terminated appropriately. The frame propagated to the right is sent to every station on the network. Each stations with physical addresses other than 87 drops the frame because the destination address in the frame does not match its own physical address.
- The intended destination computer, however, finds a match between the destination address in the frame and its own physical address. The frame is checked, the header and trailer are dropped, and the data part is decapsulated and delivered to the upper layer.

Example of Physical Address:

- Most local area networks use a 48-bit (6-byte) physical address written as 12 hexadecimal digits; every byte (2 hexadecimal digits) is separated by a colon, as shown below:

07:01:02:01:2C:4B

2. Logical Addresses (IP address):

- When source and destination are from different networks or in an internetworking environment, physical addresses are not adequate where different networks can have different address formats.

- A unique universal addressing system is needed in which every computer can be identified uniquely, regardless of the underlying physical network. The logical addresses are designed for this purpose.
- Logical addresses in a network model are necessary for universal communications that are independent of underlying physical networks.
- A logical address can uniquely define a host connected to the Internet. No two publicly addressed and visible hosts on the Internet can have the same IP addresses. Logical addresses are necessary for universal communications.
- An IP address is 32 bit address usually written in dotted decimal format A.B.C.D. where each number is in the range 0 to 255. For example, 192.9.100.2.

Example:

- Fig. 2.11 shows a part of an Internet with two routers connecting three LANs.

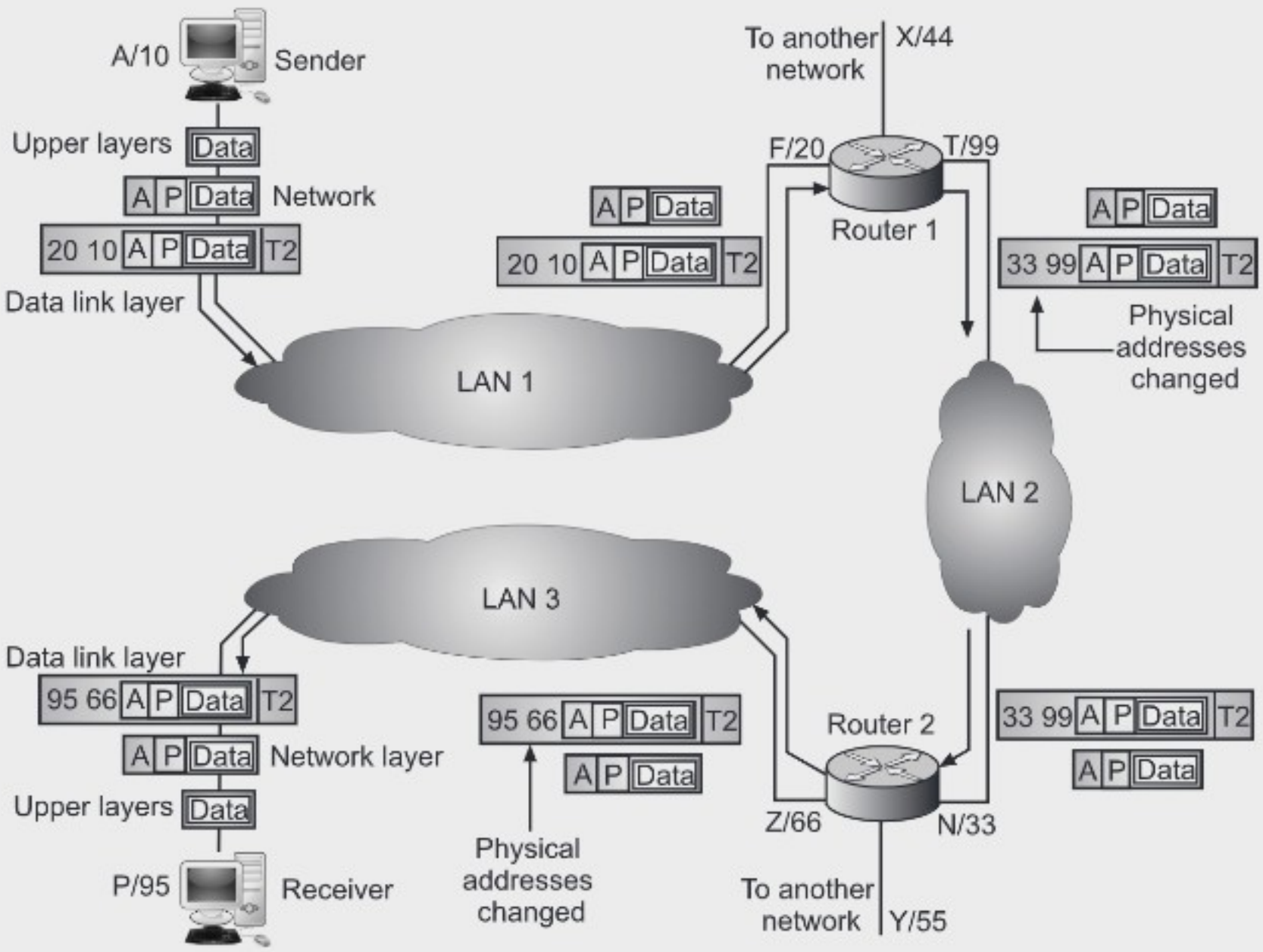


Fig. 2.11: Logical (IP) Addresses

- Each device /node like computer or router has a pair of addresses (logical and physical) for each connection. In this case, each computer is connected to only one link and therefore has only one pair of addresses.

- Each router, however, is connected to three network models for this reason each router has three pairs of addresses, one for each connection. Although it may be obvious that each router must have a separate physical address for each connection, it may not be obvious why it needs a logical address for each connection.

3. Port Addresses:

- The IP address and the physical address in a network model are necessary for a quantity of data to travel from a source host to the destination host.
- However, arrival at the destination host is not the final objective of data communications on the Internet.
- A system that sends nothing but data from one computer to another is not complete.
- Today, computers are devices that can run multiple processes at the same time. The end objective of Internet communication is a process communicating with another process.
- For example, computer x can communicate with computer z by using TELNET. At the same time, computer x communicates with computer y by using the File Transfer Protocol (FTP). For these processes to receive data simultaneously, we need a method to label the different processes. In other words, they need addresses. In the TCP/IP network model architecture, the label assigned to a process is called a port address.

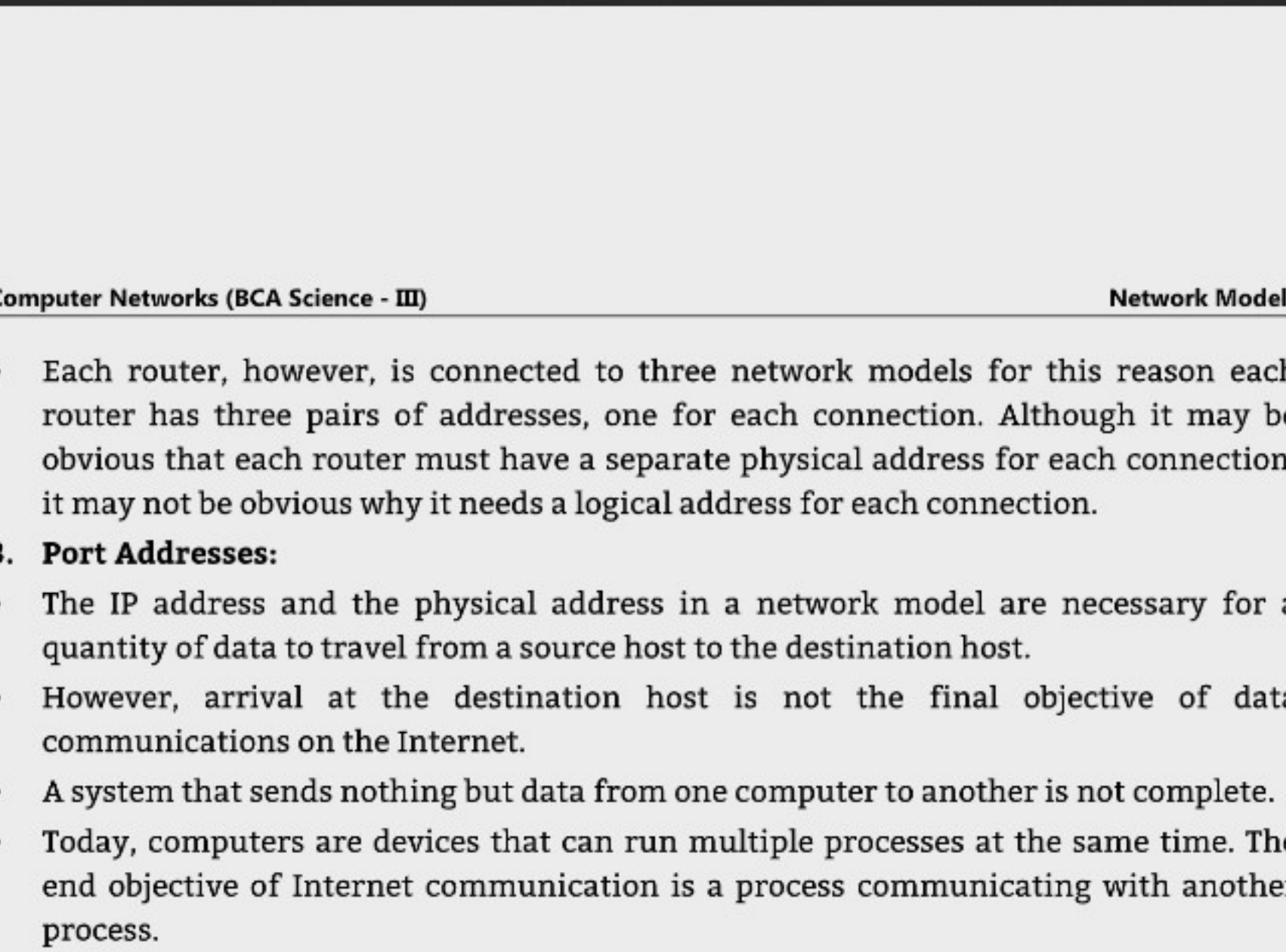


Fig. 2.12: Port Addresses

- A port address in TCP/IP network model is 16 bits in length. For example, A port address is a 16-bit address represented by one decimal number as 753.
- IANA (Internet Assigned Numbers Authority) has divided port numbers into three ranges:
  (i) **Well Known Ports:** Ports ranging from 0 to 1023 are assigned and controlled by IANA.
  (ii) **Registered Ports:** Ports from 1024 to 49,151 can be registered with IANA to prevent duplication.
  (iii) **Dynamic Ports:** Ports from 49,152 to 65,535. They can be used by any process.
- In Fig. 2.12, two computers are communicating via the Internet are shown. The sender is running three processes with port addresses x, y and z.
- The receiver is running two processes with port address a and b. Process 'x' wants to communicate with process 'a'. Both computers are using the same application. Process x's data must be delivered to process a and not b.
- For this, the transport layer encapsulates data from the application layer in a packet and adds two port addresses x and a, as source port and destination port addresses.
- The packet is then given to the network layer which adds logical addresses M and N and then the data link layer adds physical addresses of the next hop. Although physical addresses change from hop to hop, logical and port addresses remain the same.

4. **Specific Addresses:**

- Addresses are user friendly addresses and are called specific addresses.
- Some applications use friendly addresses that are designed for that specific address.
- For example, e-mail address and URL, for example: iamheremg@gmail.com, www.educationindia.edu and so on.

Summary

- A network model is a combination of hardware and software that sends data from one location to another.
- The hardware consists of the physical equipment that carries signals from one point of the network model to another. The software consists of instruction sets that make possible the services that we expect from a network model.
- Network models define a set of network layers and how they interact with each other.

- A reference model is a conceptual framework for understanding relationships.
- The International Standards Organization (ISO) has defined a standard called the Open Systems Interconnection (OSI) reference model.
- The TCP/IP model is sometimes called the DOD model since it was designed for the department of defense. It is also called the internet model because TCP/IP is the protocol used on the Internet.
- OSI reference model is a logical framework for standards for network communication. The OSI reference model is now considered as a primary standard for internetworking and internet computing.
- 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 ISO-OSI model consists of seven layer i.e. Physical Layer, Data Link Layer, Network Layer, Transport Layer, Session Layer, Presentation Layer, Application Layer.
- Physical layer activates, maintains and deactivates the physical connection. It converts the digital bits into electrical signal.
- Data link layer synchronizes the information which is to be transmitted over the data and it also provides error and flow controlling.
- The Network Layer routes the signal through different channels to the other end.
- The Transport Layer decides if data transmission should be on parallel path or single path. Functions such as multiplexing, segmenting or splitting on the data done by layer four that is transport layer.
- Session layer manages and synchronizes the conversation between two different applications.
- Presentation layer takes care that the data is sent in such a way that the receiver will understand the information (data) and will be able to use the data. Languages (syntax) can be different form the two communicating systems.
- Manipulation of data (information) in various ways is done in Application Layer. Transferring of files disturbing the results to the user is also done in this layer. Mail services, directory services, network resources etc. are services provided by the application layer.
- TCP/IP means Transmission Control Protocol and Internet Protocol. Protocols are set of rules which govern every possible communication over the Internet.

- A network address is an identifier for a node or network interface of a computer network. A network address is simply a code used by computers as a means of identification.
- Addressing is the mechanism for identifying senders and receivers, on the network.
- TCP/IP protocol suite uses four different types of addresses i.e. Physical addresses (also known as the link address, is the address of the node as defined by its LAN and WAN), Logical Addresses (also called as IP address, is a unique universal addressing system is needed in which every computer can be identified uniquely, regardless of the underlying physical network), Port addresses (a port address is a 16-bit address represented by one decimal number), Specific addresses (user friendly addresses).
- TCP/IP is also called the Internet Model. It has four layers.
- The TCP/IP is a set of protocols, or a protocol suite, that defines how all transmissions are exchanged across the Internet.

Check Your Understanding

1. Which layer of the OSI reference model corresponds to the IP protocol of the TCP/IP protocol stack?
   (a) Transport (b) Network
   (c) Internet (d) Data link.
2. The entities in the same layer on different machines are called _____.
   (a) Hosts (b) Peers
   (c) Protocols (d) IMP's.
3. As the data packet moves from the lower to the upper layers, headers are _____.
   (a) Added (b) Rearranged
   (c) Modified (d) Subtracted
4. Which of the following is a TCP/IP transport layer protocol?
   (a) IP (b) FTP
   (c) UDP (d) ICMP.
5. What is the main function of the transport layer ?
   (a) Process-to-process delivery (b) Note-to-node delivery
   (c) Synchronization (d) Updating and maintenance of routing tables.

6. Which of the following device operates at the network layer of the OSI model?
   (a) Repeater (b) Router
   (c) Bridge (d) Hub.
7. The length of an IP address is _____ bits.
   (a) 46 (b) 32
   (c) 16 (d) 64.
8. Which of the following is a NOT an Internet layer protocol in the TCP/IP stack?
   (a) IP (b) UDP
   (c) ARP (d) ICMP.

ANSWER KEY

1. (b)	2. (b)	3. (d)	4. (c)	5. (a)
6. (b)	7. (b)	8. (b)		

Practice Questions

Q.1: Answers the Following Questions in short.

1. What is meant by reference model?
2. What is interface and peers?
3. What do you mean by OSI?
4. What are the seven layers of ISO's OSI model?
5. What are the key functions of data link layer?

Q.2: Answers the Following Questions.

1. Write a note on the TCP/IP reference model with neat diagram.
2. Compare and contrast OSI and TCP/IP reference model.
3. Explain different levels of addresses used in networks.
4. Write a note on TCP/IP model.
5. What is the structure of a physical, IP, port and specific address ?
6. What are the function of each layer of OSI model?
7. Explain TCP/IP protocol suite diagrammatically.
8. Explain Addressing in detail.

Q.3: Define the following terms.

1. Physical address
2. Network model
3. Peers
4. Encapsulation
5. De-encapsulation

Previous Exam Questions

Summer 2019

1. Which of the following device operators is at the network layer of OSI model? **[1 M]**

(i) Router
(ii) Repeater
(iii) Bridge
(iv) None of the above

2. Which of the layer is not network support layer ? **[1 M]**

(i) Network layer
(ii) Physical layer
(iii) Transport layer
(iv) None of the above

3. List the layers of OSI. **[1 M]**

Ans. Refer to section 2.2

4. Compare TCP/IP and OSI model. **[5 M]**

Ans. Refer to section 2.5

Winter 2018

1. As data pockets move from lower to upper layers, headers are: **[1 M]**

(i) Added
(ii) Modified
(iii) Rearranged
(iv) Subtracted

2. What is meant by reference model. **[1 M]**

Ans. Refer to section 2.2

3. List the network layer services. **[1 M]**

Ans. Refer to section 2.2.1

4. Give the function of physical layer. **[4 M]**

Ans. Refer to section 2.2.1

5. Write a short note on TCP/IP model. **[3 M]**

Ans. Refer to section 2.3

Summer 2018

1. Which layer of the OSI reference model corresponds to the IP protocol of the TCP/IP protocol stack ? **[1 M]**

(a) Transport

(b) Network

(c) Internet

(d) Data link.

2. Compare and contrast OSI and TCP/IP reference model. **[5 M]**

Ans. Refer to section 2.5

❖❖❖

3... Physical Layer

Objectives...

- To understand Functionality of Physical Layer.
- To understand Basic Concept of Signals.
- To understand Various Transmission Impairments.
- To study Measures for Performance of Network.
- To learn different Line Coding Schemes to convert Data into Signals.
- To study different Transmission Modes.
- To understand various Multiplexing and Switching Techniques.

3.1 INTRODUCTION

- The physical layer is concerned with transmission of raw bits over a communication channel.
- It specifies the mechanical, electrical and procedural network interface specifications and the physical transmission of bit streams over a transmission medium connecting two pieces of communication equipment.
- Physical layer which actually interacts with transmission media, which connects network components together.
- Physical layer involved in physically carrying information from one node in the network to the next.
- The Physical layer performs complex tasks. It provides services to the Data link layer. The data in the Data link layer is organized in 0's and 1's in smaller frames. These streams of 0's and 1's must be converted into signals. One of the services provide by the physical layer is to create a signal that represents this stream of bits.
- The Physical layer must also take care of the transmission medium. The transmission medium must be controlled by the physical medium.
- Physical layer decides on the direction of data flow. It decides on the number of logical channels for transporting data coming from different sources.

3.2 BASIC CONCEPTS OF SIGNALS

- Data refers to information that conveys some meaning based on some mutually agreed up rules or conventions between a sender and a receiver and today it comes in a variety of forms such as text, graphics, audio, video and animation.
- Signal is an electrical, electronic or optical representation of data, which can be sent over a communication medium.
- A signal can be represented as a function of time and frequency. In mathematical terms, a signal is merely a function of the data.
- Both data and the signals that represent them can be either analog or digital in form.

3.2.1 Analog and Digital Data

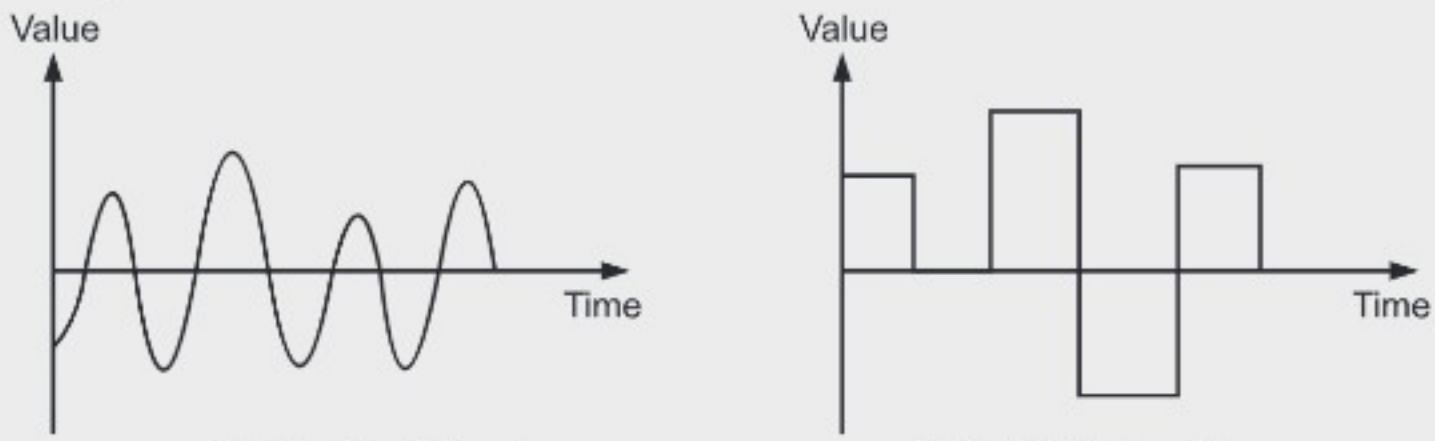
Analog and Digital Data:

- Data can be analog or digital.
- Analog data are continuous values. For example, a human voice or analog clock that has hour, minute and second hands give information in a continuous form. The movements of the hands are continuous.
- Digital data have discrete states and take discrete values. For example, data stored in a computer or digital clock that changes suddenly from 10.10 to 10.11.

3.2.2 Analog and Digital Signals (W-18)

Analog and Digital Signals:

- Signals can be either analog or digital as shown in Fig 3.1.
- Analog signals can have an infinite number of values in a range. As the wave moves from value A to value B, it passes through and includes an infinite number of values along its path.
- Digital signals can have only a limited number of defined values. Although each value can be any number, it is like 1 and 0.

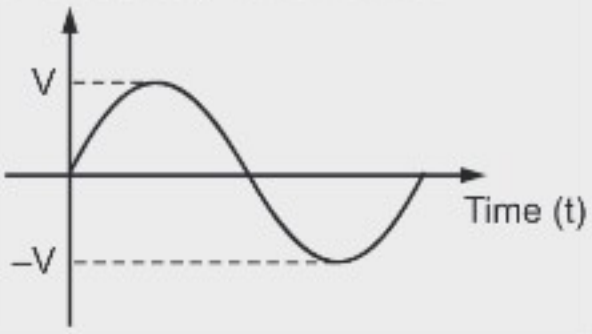
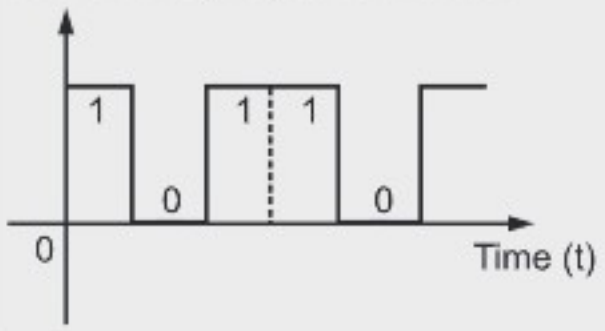


(a) Analog Signal **(b) Digital Signal**

Fig. 3.1: Analog and Digital Signals

- Digital transmission has advantages over analog transmission in many ways.
  1. A digital signal can pass through a number of repeaters without loss of signal and so travel long distances without loss of data, whereas analog signals lose the data when amplified.
  2. Higher data rates are possible in digital transmission by using existing lines which are not in analog.
  3. In digital, we can integrate voice, data, video and music.
  4. Easier to multiplex large channel capacities with digital.
  5. Easy to apply encryption to digital data.
  6. Maintenance is easier in digital transmission than analog.
  7. Nowadays, the cost of digital equipment and size is continuously reducing, so digital transmission becomes cheaper than analog.
- Following Table shows difference between Analog and Digital signal.

Table 3.1: Difference between Analog Signal and Digital Signal

Terms	Analog signal	Digital signal
1. Signal	Analog signal is a continuous signal which represents physical measurements.	Digital signals are discrete time signals generated by digital modulation.
2. Waves	Denoted by sine waves: 	Denoted by square waves: 
3. Representation	Uses a continuous range of values to represent information.	Uses discrete or discontinuous values to represent information.
4. Example	Human voice in air, analog electronic devices.	Computers, CDs, DVDs, and other digital electronic devices.
5. Flexibility	Analog hardware is not flexible.	Digital hardware is flexible in implementation.
6. Uses	Can be used in analog devices only. Best suited for audio and video transmission.	Best suited for Computing and digital electronics.

7.	Applications	Thermometer	PCs, PDAs
8.	Power	Analog instruments draw large power.	Digital instruments draw only negligible power.
9.	Cost	Low cost and portable.	Cost is high and not easily portable.
10.	Impedance	Low.	High.

3.2.3 Digital Signals - Bit Rate, Bit Length (S-18, 19)

- A digital signal used to represent data.
- Most digital signals are non-periodic and thus, period or frequency is not appropriate. Two new terms, bit interval and bit rate are used to describe digital signals instead of period and frequency respectively.
  - **Bit Interval:** The bit interval is the time required to send one single bit.
  - **Bit Rate:** The bit rate is the number of bit intervals per second. This means that the bit rate is the number of bits sent in one second, usually expressed in bits per second (bps) as shown in Fig. 3.2.
  - **Bit Length:** For analog signal, the distance one cycle occupies on the transmission medium is called wavelength. Similarly for a digital signal, the bit length is used. The bit length is the distance one bit occupies on the transmission medium.

Bit length = propagation speed × bit duration

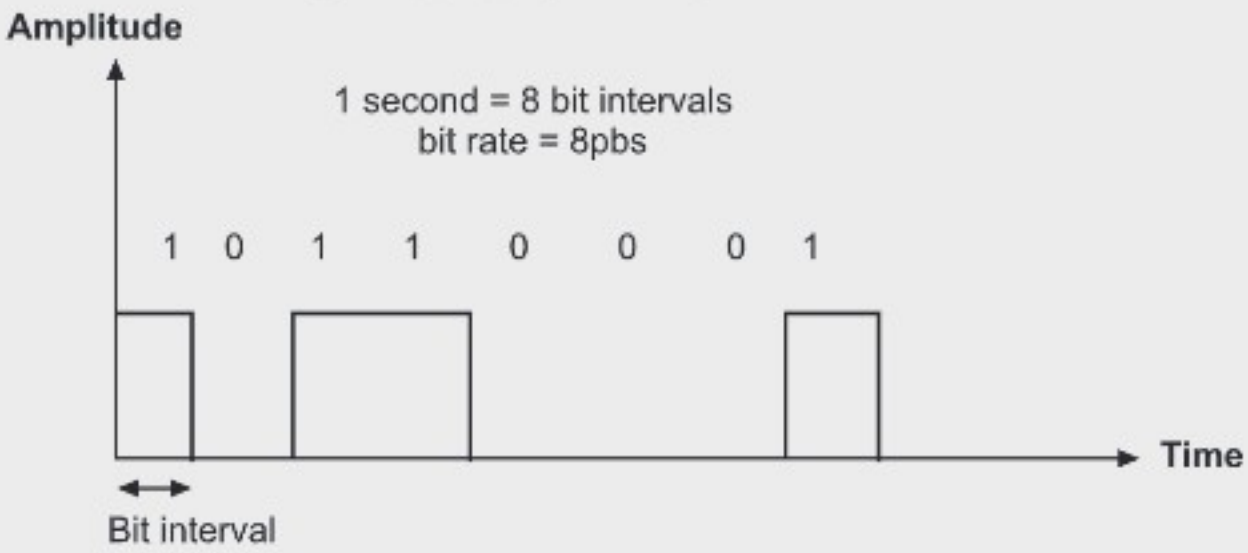


Fig. 3.2: Bit Rate and Bit Interval

Example 1: A digital signal has eight levels. How many bits are needed per level?

Solution: We calculate the number of bits from the formula:

Number of bits per level = $\log_2 L = \log_2 8 = 3$

Therefore, each signal level is represented by 3 bits.

3.3 TRANSMISSION OF DIGITAL SIGNALS

- We can transmit a digital signal by using baseband transmission or broadband transmission (using modulation).

3.3.1 Baseband Transmission

- Baseband transmission means sending a digital signal over a channel without changing the digital signal to an analog signal.
- Baseband transmission requires low pass channel, a channel with a bandwidth that starts from zero.
- So Baseband communication has two cases: a low pass channel with a wide bandwidth and one with a limited bandwidth.

1. **Low pass channel with a wide bandwidth:** If we want to preserve the exact form of a non-periodic digital signal with vertical segments vertical and horizontal segments horizontal, we need to send the entire spectrum, the continuous range of frequencies between zero and infinity. This is possible if we have a dedicated medium with an infinite bandwidth between the sender and receiver that preserves the exact amplitude of each component of the composite signal. Thus Baseband transmission of a digital signal that preserves the shape of the digital signal is possible only if we have a low-pass channel with an infinite or very wide bandwidth.
2. **Low pass channel with a limited bandwidth:** In a low-pass channel with limited bandwidth, we approximate the digital signal with an analog signal. The level of approximation depends on the bandwidth available. The required bandwidth is proportional to the bit rate. If we need to send bits faster, we need more bandwidth.

Baseband systems extend only to limited distances because at higher frequency, the attenuation of the signal is most pronounced and the pulses blur out, causing the large distance communication totally impractical.

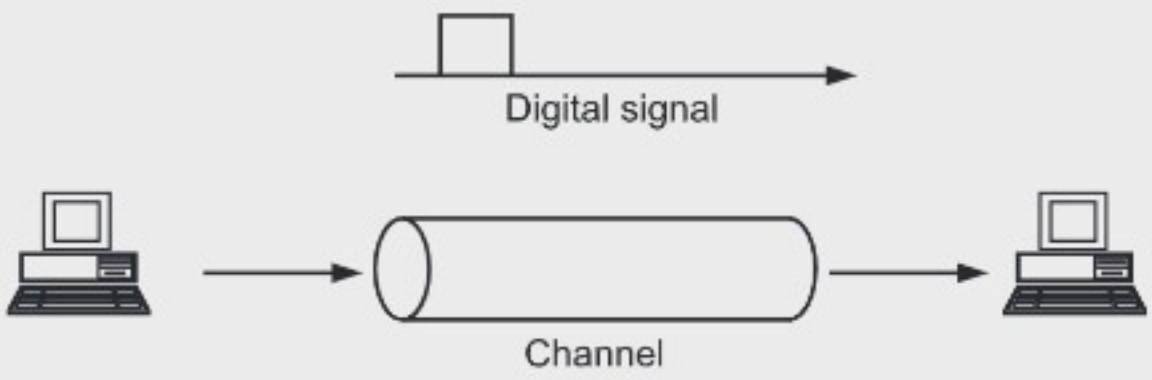


Fig. 3.3: Baseband Transmission

3.3.2 Broadband Transmission

- Broadband transmission or modulation means changing the digital signal to an analog signal for transmission.
- Modulation allows us to use a band pass channel.
- Bandwidth of the band pass channel does not start from zero. This type of channel is more available than a low-pass channel.

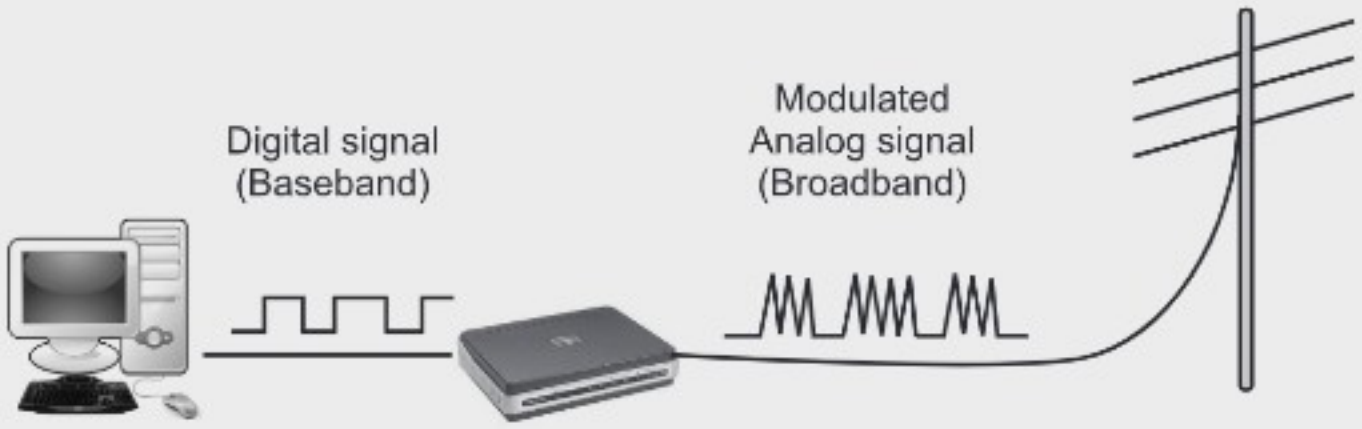


Fig. 3.4: Broadband Transmission

- If the available channel is a band pass channel, we cannot send the digital signal directly to the channel. We need to convert the digital signal to an analog signal before transmission.

3.4 TRANSMISSION IMPAIRMENTS

- When a signal is transmitted over a communication channel, it is subjected to different types of impairments because of imperfect characteristics of the channel. As a consequence, the received and the transmitted signals are not the same. Outcome of the impairments are manifested in two different ways in analog and digital signals.
- These impairments introduce random modifications in analog signals leading to distortion. On the other hand, in case of digital signals, the impairments lead to error in the bit values.
- Impairments of a signal means that the signal quality at the beginning of the medium is not the same as that at the end.
- The impairment can be broadly categorized into the following three types as shown in Fig. 3.5, i.e. attenuation, distortion and noise.

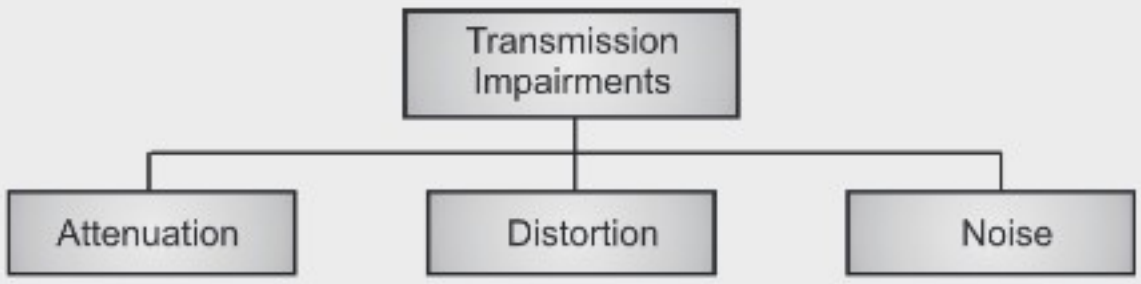


Fig. 3.5: Causes of Impairments

3.4.1 Attenuation

- Attenuation means a loss of energy and the resistance of the medium.
- When a signal travels through a medium, it loses some of its energy in overcoming the resistance of the medium.
- Irrespective of whether a medium is guided or unguided, the strength of a signal falls off with distance. In case of guided media, the attenuation is logarithmic, whereas in case of unguided media it is a more complex function of the distance and the material that constitutes the medium.

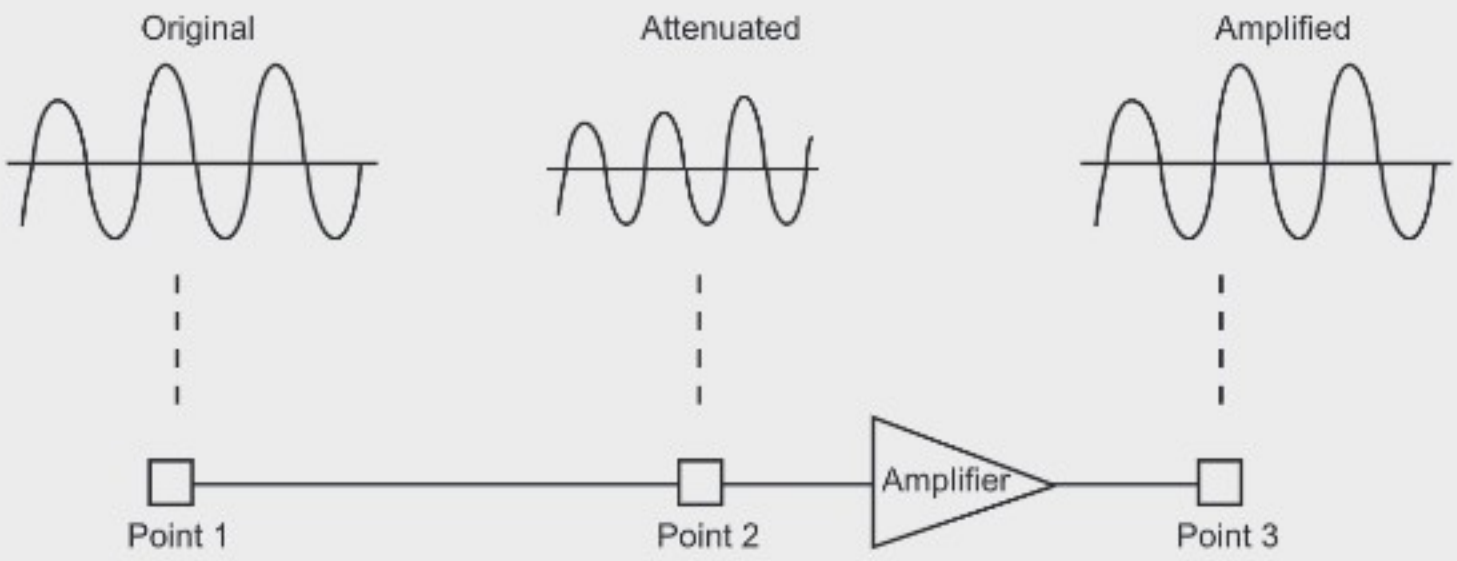


Fig. 3.6: Effect of Attenuation and Amplification

- To compensate for the loss of signals, amplifiers are used to amplify the signal.
- Fig. 3.6 shows the effect of attenuation and amplification.
- To show that a signal has lost or gained strength, unit decibel is used. The decibel (dB) measures the relative strengths of two signals or one signal at two different points.

$$dB = 10 \log_{10} \frac{P_2}{P_1}$$

- Variables P_1 and P_2 are the powers of a signal at points 1 and 2, respectively.
- The decibel is negative if a signal is attenuated and positive if a signal is amplified.

Example 2: Suppose a signal travels through a transmission medium and its power is reduced to one-half. What will be attenuation?

Solution: P_2 is $(1/2)P_1$.

So the attenuation (loss of power) can be calculated as below:

$$10 \log_{10} \frac{P_2}{P_1} = 10 \log_{10} \frac{0.5\, P_1}{P_1} = 10 \log_{10} 0.5 = 10(-0.3) = -3 \text{ dB}$$

A loss of 3 dB (–3 dB) is equivalent to losing one-half the power.

3.4.2 Distortion

- Distortion is the alteration of a signal due to the differing propagation speeds of each of the frequencies that makeup a signal.
- The signal changes its form or shape. Distortion can occur in a composite signal made of different frequencies. Each signal component has its own propagation speed through a medium and therefore its own delay in arriving at the destination.
- Signal components at the receiver have phases different from what they had at the sender. So the shape of the composite signal is not the same.
- Fig. 3.7 shows the effect of distortion on a composite signal.

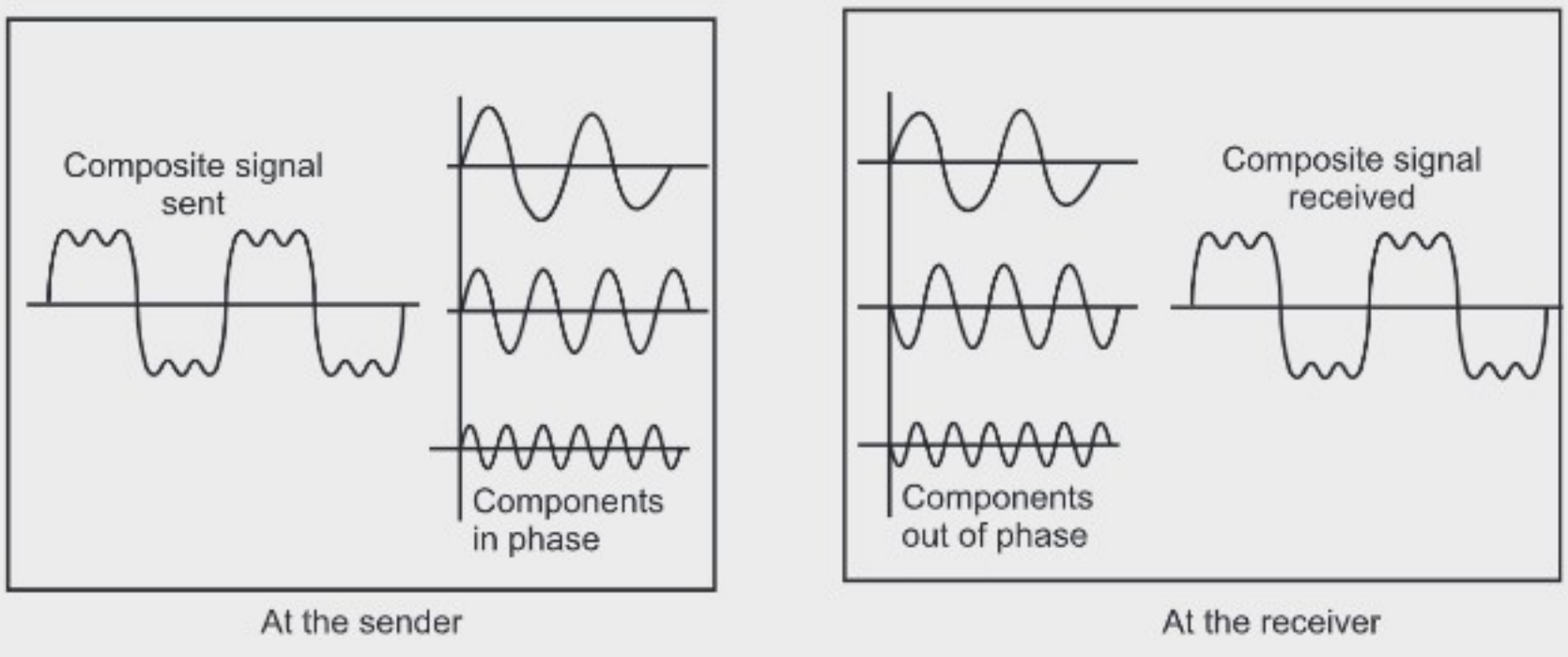


Fig. 3.7: Effect of Distortion on a Composite signal

3.4.3 Noise (W-18)

- Noise is the external energy that corrupts a signal
- As signal is transmitted through a channel, undesired signal in the form of noise gets mixed up with the signal, along with the distortion introduced by the transmission media.
- Noise can be categorized into the following four types as described below:
  1. Thermal noise is the random motion of electrons in a wire which creates an extra signal, not sent by the transmitter. It is also known as white noise.
  2. Induced noise created by motors and appliances. These devices act as a sending antenna, and the transmission medium acts as the receiving antenna.
  3. Crosstalk is the effect of one wire on the other. In other words, it is a result of bunching several conductors together in a single cable. Signal carrying wires generate electromagnetic radiation, which is induced on other conductors because of close proximity of the conductors. While using the telephone, it is a common experience to hear conversation of other people in the background. This is known as cross talk.

4. Impulse noise is irregular pulses or noise spikes of short duration generated by phenomena like lightning, spark due to loose contact in electric circuits, etc. Impulse noise is a primary source of bit-errors in digital data communication. This kind of noise introduces burst errors.

- Fig. 3.8 shows effect of noise on a signal.

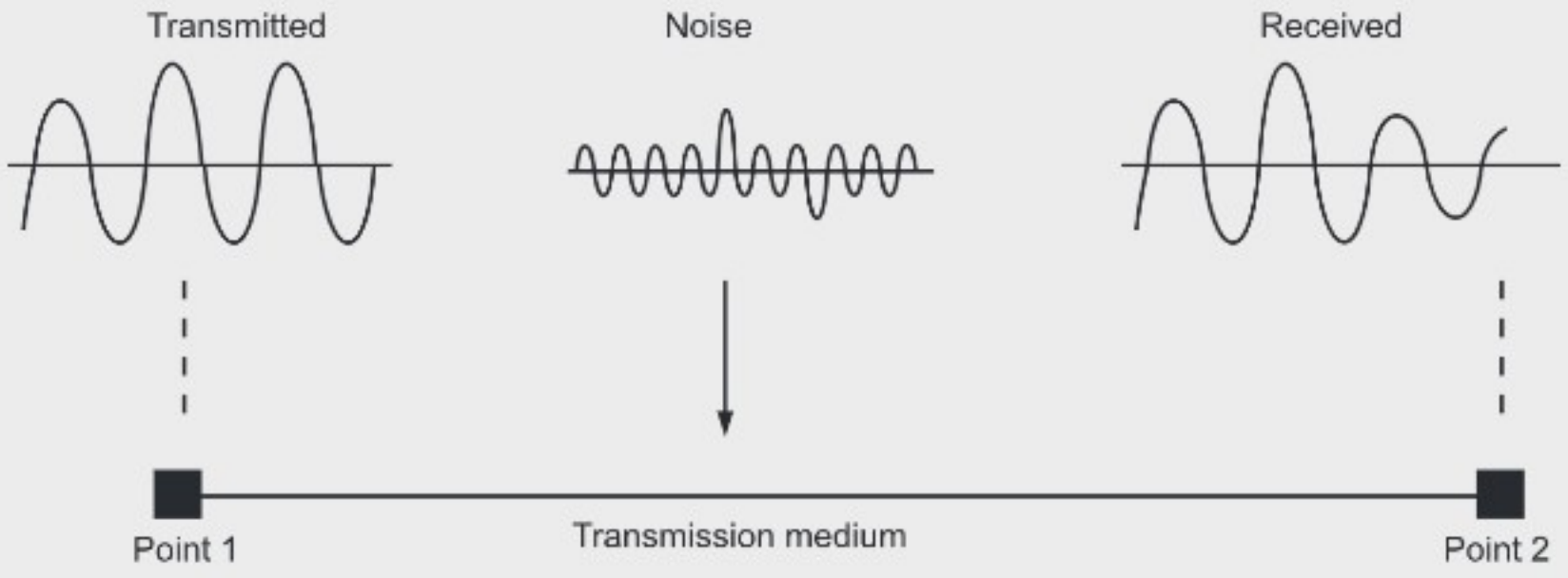


Fig. 3.8: Effect of Noise on a signal

3.5 DATA RATE LIMITS

- In data communication, a very important consideration is how fast we can send data, in bits per second, over a channel. Data rate depends upon:
  1. The bandwidth available,
  2. The level of the signals we use, and
  3. The quality of the channel (the level of noise).
- The maximum rate at which data can be correctly communicated over a channel in presence of noise and distortion is known as its channel capacity.
- Two formulas were developed to calculate the data rate:
  1. Nyquist for a noiseless channel.
  2. Shannon for a noisy channel.

3.5.1 Noiseless Channel: Nyquist Bit Rate

Nyquist Bit Rate formula for Noiseless Channel:

- For a noiseless channel, the Nyquist bit rate formula defines the theoretical maximum bit rate.

  $$\text{Bit rate} = 2 \times \text{bandwidth} \times \log_2 L$$

- Bandwidth is the bandwidth of the channel. L is the number of signal levels used to represent data.
- Bit rate is the bit rate in bits per second.
- Practically, there is a limit on bit rate. Increasing the levels of a signal may reduce the reliability of the system.

Example 3: Consider a noiseless channel with a bandwidth of 4000 Hz transmitting a signal with two signal levels. What will be the maximum bit rate?

Solution:

$$\text{Bit Rate} = 2 \times \text{bandwidth} \times \log_2 L$$
$$= 2 \times 4000 \times \log_2 2$$
$$= 8000 \text{ bps.}$$

Example 4: We need to send 265 kbps over a noiseless channel with a bandwidth of 20 kHz. How many signal levels do we need?

Solution:

$$\text{Bit Rate} = 2 \times \text{bandwidth} \times \log_2 L$$
$$265{,}000 = 2 \times 20{,}000 \times \log_2 L$$
$$\text{Log}_2 L = 6.625$$
$$L = 2^{6.625}$$
$$L = 98.7 \text{ levels}$$

Example 5: Let us consider the telephone channel having bandwidth B = 4 kHz. Assuming there is no noise, determine channel capacity for the encoding levels-128.

Solution:

$$\text{Bit Rate} = 2 \times \text{bandwidth} \times \log_2 L$$
$$= 2 \times 4000 \times \log_2 128$$
$$= 8000 \times 7 = 56 \text{ Kbits/s}$$

3.5.2 Noisy Channel : Shannon's Law

Shannon's Law for Noisy Channel:

- In reality, we cannot have a noiseless channel, the channel is always noisy. When there is noise present in the medium, the limitations of both bandwidth and noise must be considered.
- A noise spike may cause a given level to be interpreted as a signal of greater level, if it is in positive phase or a smaller level, if it is negative phase. Noise becomes more problematic as the number of levels increases.
- In 1994, Shannon introduced a formula, called Shannon capacity, to determine the theoretical highest data rate for noisy channels.

$$\text{Capacity} = \text{Bandwidth} \times \text{Log}_2 (1 + \text{SNR})$$

- Bandwidth is bandwidth of the channel. SNR is signal to noise ratio, capacity is the capacity of the channel in bits per second.
- Signal to noise ratio (SNR) is calculated as,

$$\text{SNR} = \frac{\text{average signal power}}{\text{average noise power}}$$

Example 6: Calculate the theoretical highest bit rate of a regular telephone line. A telephone line normally has a bandwidth of 3000 Hz assigned for data communication. The signal to noise ratio is usually 3162. Calculate the capacity.

Solution: $C = B \log_2 (1 + SNR)$

$= 3000 \log_2 (1 + 3162)$

$= 3000 \log_2 3163$

$= 3000 \times 11.62$

Capacity $= 34860$ bps

Example 7: The digital signal is to be designed to permit 160 kbps for a bandwidth of 20 KHz. Determine (a) number of levels and (b) S/N ratio.

Solution:

(a) Apply Nyquist Bit Rate to determine number of levels.

$C = 2B \log_2 (L)$,

$160 \times 10^3 = 2 \times 20 \times 10^3 \log_2(L)$

$\log_2 (L) = 4$

$L = 24$, which means 4bits/baud.

(b) Apply Shannon capacity to determine the S/N ratio

$C = B \log_2 (1 + S/N)$,

$160 \times 10^3 = 20 \times 10^3 \log_2 (1 + S/N)$

$\log_2(1 + S/N) = 8$

$S/N = 2^8 - 1$

$S/N = 255$

$S/N = 24.07$ dB.

Example 8: Given a channel with an intended capacity of 20 Mbps. The bandwidth of the channel is 3MHz. What signal to noise ratio is required in order to achieve this capacity? **(W-18, S-19)**

Solution: According to Shannon's Capacity formula, the maximum channel capacity (in bps) is given by the equation:

$C = B \log_2 (1 + SNR)$

Where B is the bandwidth and SNR is the signal-to-noise ratio.

Given $B = 3$ MHz $= 3 \times 10^6$ Hz, and $C = 20$ Mbps $= 20 \times 10^6$ bps,

So, $20 \times 10^6 = 3 \times 10^6 \log_2 (1 + SNR)$

$\log_2 (1 + SNR) = 20 / 3 = 6.667$

$1 + SNR = 102$

Hence, $SNR = 101$

Example 9: What is the channel capacity for a teleprinter channel with a 300 Hz bandwidth and a signal to noise ratio of 3 DB?

Solution:

From the given details we know,

B (Bandwidth) = 300 Hz

SNRdb (Signal-to-noise ratio decibel) = 3 dB.

Suppose, C = Channel capacity and SNR = signal-to-noise ratio.

Now using decibel formula,

SNR db = 10 * log (SNR)

That means,

$$3 = 10 * \log (SNR)$$

$$SNR = \log^{-1} 0.3$$

$$SNR = 10^{0.3}$$

$$SNR = 1.995$$

Hence, signal-to-noise ration (SNR) = 1.995

Now using Shannon's equation,

$$C = B * \log_2(1+SNR)$$

$$C = 300 * \log_2(1+1.995)$$

$$C = 300 * \log_2(2.995)$$

$$C = 474.76$$

Therefore, the channel capacity for teleprinter channel is 474.76 bits per second.

3.6 PERFORMANCE OF NETWORK (W-18)

- One important issue in networking is the performance of the network. Performance of the network depends upon several factors, they are:
  1. Bandwidth,
  2. Throughput,
  3. Latency (delay),
  4. Bandwidth-delay product and
  5. Jitter.

3.6.1 Bandwidth (S-19)

- One characteristic that measures network performance is bandwidth.
- In networking, we use the term bandwidth in two contexts.
  1. **Bandwidth in hertz:** Bandwidth in hertz refers to the range of frequencies in a composite signal or the range of frequencies that the channel can pass.
  2. **Bandwidth in bits per second:** Bandwidth in bits per second refers to the speed of bit transmission in a channel or link.

- **Relationship:** There is an explicit relationship between in hertz and bandwidth in bits per seconds. An increase in bandwidth in hertz means an increase in bandwidth in bits per second.

3.6.2 Throughput

- The throughput is a measure of how fast we can actually send data through a network.
- Bandwidth in bits per second and throughput seem to be same, but they are different. Throughput is controlled by available bandwidth.
- A link may have bandwidth of B bps, but we can only send T bps through this link with T always less than B. Bandwidth is a potential measurement of a link and throughput is an actual measurement of how fast we can send data.
- Consider a highway designed to transmit 1000 cars per minute from one point to another. However, if there is congestion on the road, this can be reduced to 200 cars per minute. So bandwidth is 1000 cars per minute and throughput is 200 cars per minute.

Example 10: A network with bandwidth of 10 Mbps can pass only an average of 12,000 frames per minute with each frame carrying an average of 10,000 bits. What is the throughput of this network?

Solution:
$$\text{Throughput} = \frac{12{,}000 \times 10{,}000}{60}$$
$$= 2 \text{ Mbps}$$

3.6.3 Latency (Delay)

- The latency or delay defines how long it takes for an entire message to completely arrive at the destination from the time the first bit is sent out from the source.

Latency = Propagation time + Transmission time + Queuing time + Processing delay

Propagation Time:

- Propagation time measures the time required for a bit to travel from the source to destination.

$$\text{Propagation time} = \frac{\text{Distance}}{\text{Propagation speed}}$$

Example 11: What is the propagation time if the distance between the two points is 12,000 km. Assume the propagation speed to be 2.4×10^8 m/s in cable.

Solution:
$$\text{Propagation time} = \frac{12{,}000 \times 1000}{2.4 \times 10^8}$$
$$= 50 \text{ ms}$$

Transmission Time:

- In data communication, a message containing bits is sent. The first bit may take a time equal to the propagation time to reach its destination; the last bit also may take the same amount of time.
- However, there is a time between the first bit leaving the sender and the last bit arriving at the receiver. The first bit leaves earlier and arrives earlier, the last bit leaves later and arrives later. The time required for transmission of a message depends on the size of the message and the bandwidth of the channel.

$$\text{Transmission time} = \frac{\text{Message size}}{\text{Bandwidth}}$$

Example 12: What is the propagation time for a 2.5 kbyte message if the bandwidth of the network is 1Gbps? Assume that the distance between the sender and the receiver is 12,000 km and that light travels at 2.4×10^8 m/s.

Solution:

$$\text{Propagation time} = \frac{12000 \times 1000}{2.4 \times 10^8}$$

$$= 50 \text{ ms}$$

$$\text{Transmission Time} = \frac{2500 \times 8}{10^9}$$

$$= 0.020 \text{ ms}$$

Queuing Time:

- The third component in latency is the queuing time, the time needed for each intermediate or end device to hold the message before it can be processed.
- The queuing time is not fixed, it depends upon the load on the network. When there is heavy traffic on the network, the queuing time increases.

3.6.4 Bandwidth-Delay Product

- By Bandwidth and delay, we measure the performance of a network. In data communication, the product of bandwidth and delay is very important.
- Let us elaborate this issue, using two hypothetical cases as examples.

Case 1:

- Let us consider that we have a link with a bandwidth of 1bps and the delay of the link is 5s. From the Fig. 3.9 we can say that bandwidth delay product is 1 × 5, is the maximum number of bits that can fill the link. There can be no more than 5 bits at any time on the link.

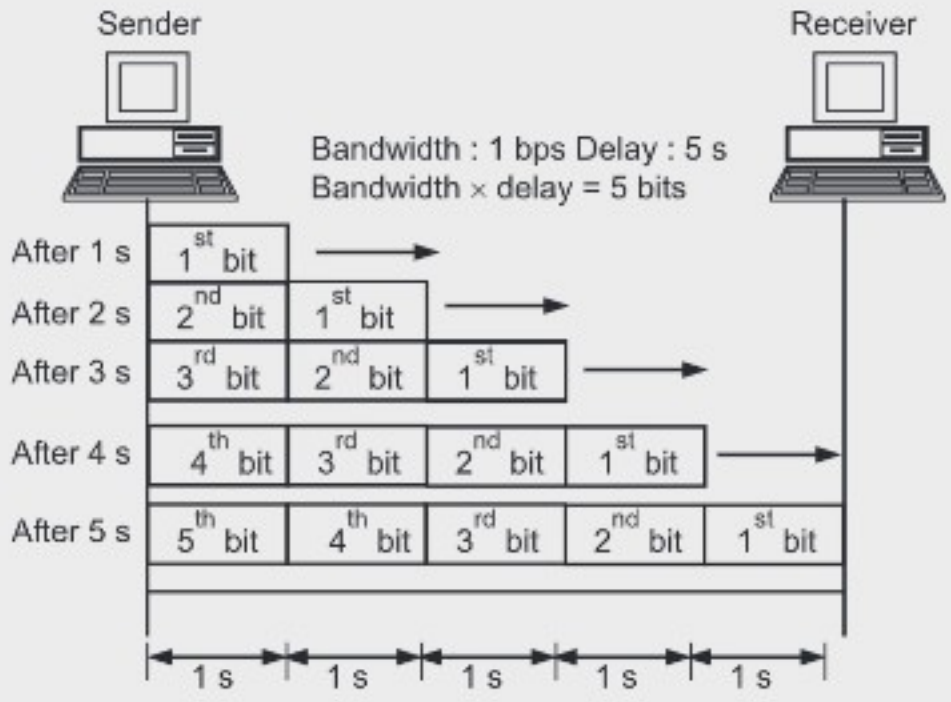


Fig. 3.9: Filling the Link with Bits for Case 1

Case 2:

- Now, assume we have a bandwidth of 4bps. Fig. 3.10 shows there can be 4 × 5 = 20 bits on the line. At each second, there are 4 bits on the line, the duration of each bit is 0.25s.

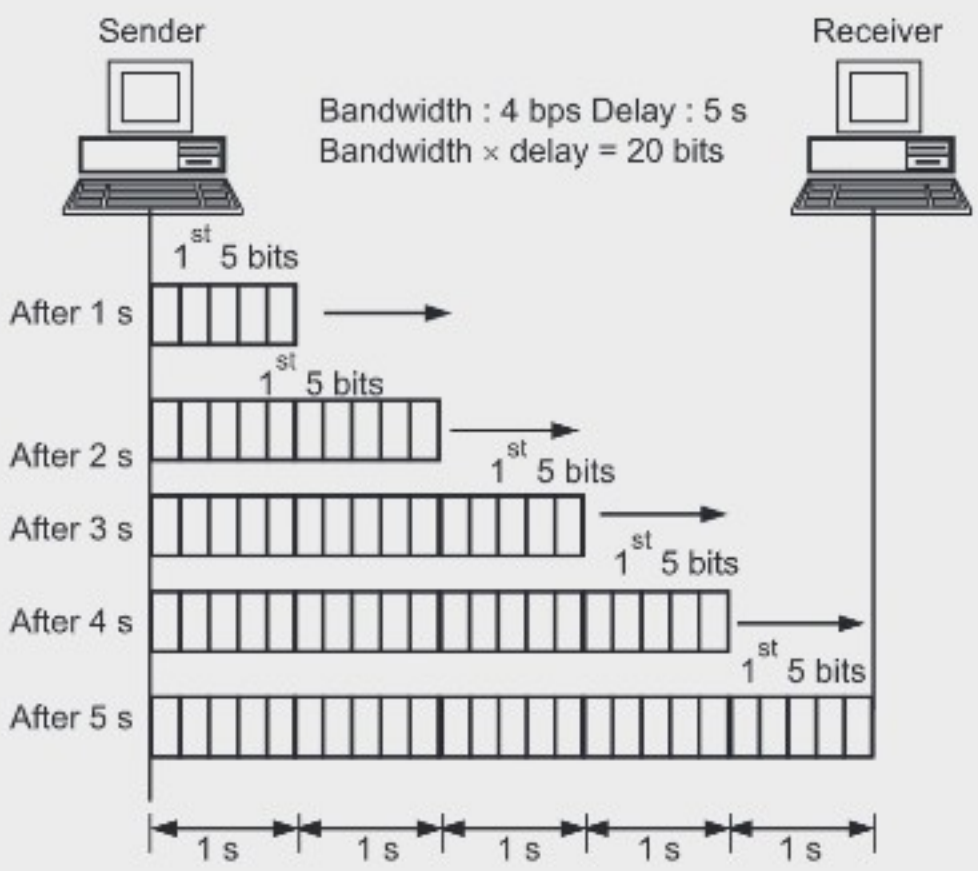


Fig. 3.10: Filling the Link with Bits in Case 2

- The above two cases show that the product of bandwidth and delay is the number of bits that can fill the link.

3.6.5 Jitter (S-19)

- Another performance issue that is related to delay is jitter. We can roughly say that jitter is a problem if different packets of data encounter different delays and the application using the data at the receiver site is time-sensitive (audio and video data, for example).
- If real-time data (audio/video) on a packet switched network requires the preservation of the time relationship between packets of a session. For example, consider a server sending 3 packets to client. Every packet contains 10S video information.
- The first packet starts at 00.00.00, the second at 00.00.10 and the third at 00.00.20. Also consider 1s is required for every packet to reach upto destination. The receiver can play the first packet at 00:00:01, the second at 00:00:11 and the third at 00:00:21.
- Fig. 3.11 shows this idea.

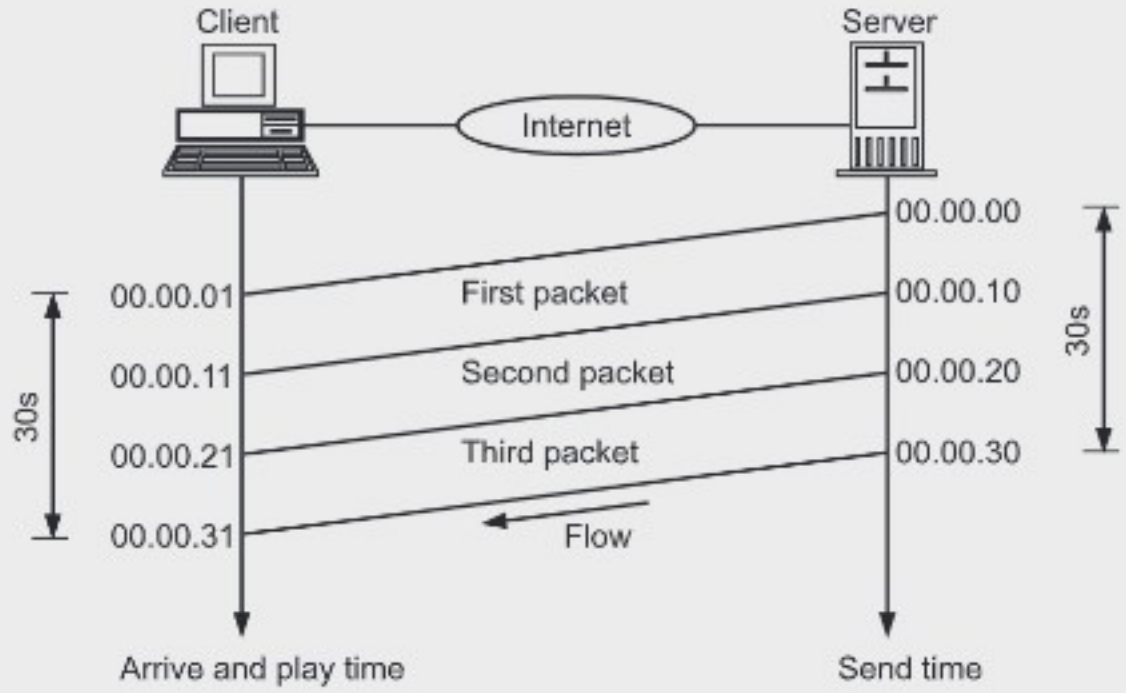


Fig. 3.11 Real time data Transfer on packet Switch network

- But if the first packet arrives at 00:00:01 (1s delay), the second arrives at 00:00:15 (5s delay), and the third arrives at 00:00:27 (7s delay) the receiver is not able to play packets.
- After playing the first packet, he has to wait for the second. There is a gap between the first and second packets and between second and third as the video is viewed at the remote site.
- This concept is called jitter and shown in Fig. 3.12.
- A computer network is designed to send information from one point to another. This information needs to be converted either into digital signal or analog signal for transmission.

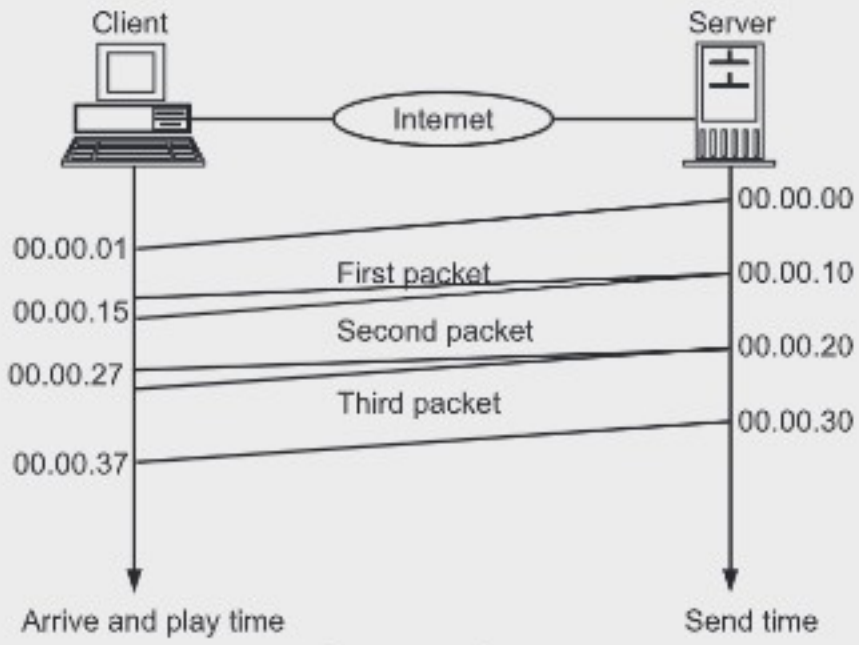


Fig. 3.12: Jitter

3.7 LINE CODING

- Line coding is the process of converting digital data to digital signals. Line coding converts the sequence of bits to a digital signal.
- At the sender, digital data are encoded into a digital signal, at the receiver; the digital data are recreated by decoding the digital signal.

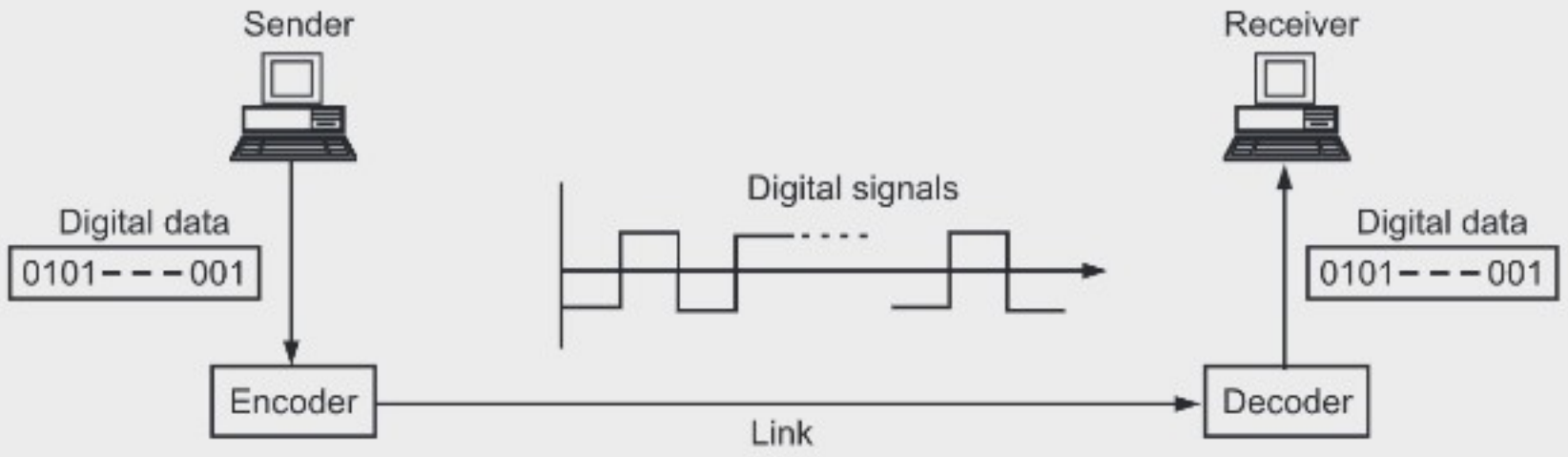


Fig. 3.13: Line Coding and Decoding

3.7.1 Line Coding Characteristics (S-18, 19)

- The common characteristics of line coding are:
  1. **Signal element versus Data element:** A data element is the smallest entity that can represent a piece of information, this is the bit. In digital data communications, a signal element carries data elements. A signal element is the shortest unit of a digital signal. Data elements are being carried, signal elements are the carriers.
  2. **Data rate versus signal rate:** The data rate defines the number of data elements (bits) sent in 1s. The signal rate is the number of signal elements sent in 1s.
  3. **Bandwidth:** Although the actual bandwidth of a digital signal is infinite, the effective bandwidth is finite.

4. **Baseline wandering:** In decoding a digital signal, the receiver calculates a running average of the received signal power. This average is called the baseline. A long string of 0s or 1s can cause a drift in the baseline is called baseline wandering.
5. **DC Components:** When the voltage level in a digital signal is constant for a while, the spectrum creates very low frequencies. These frequencies around zero are called DC components. DC component in a signal is not desirable because the DC component does not pass through some components of a communication system such as a transformer. This leads to distortion of the signal and may create error at the output. The DC component also results in unwanted energy loss on the line.
6. **Signal Spectrum**: Different encoding of data leads to different spectrum of the signal. It is necessary to use suitable encoding technique to match with the medium so that the signal suffers minimum attenuation and distortion as it is transmitted through a medium.
7. **Self Synchronization:** To correctly interpret the signals received from the sender, the receiver's bit intervals must correspond exactly to the sender's bit intervals. If the receiver clock is faster or slower, the bit intervals are not matched and the receiver might misinterpret the signals. Usually, a clock is generated and synchronized from the received signal with the help of a special hardware known as Phase Lock Loop (PLL). However, this can be achieved if the received signal is self-synchronizing, having frequent transitions (preferably, a minimum of one transition per bit interval) in the signal. A self synchronizing digital signal includes timing information in the data being transmitted.
8. **Built in error detection:** There should be built in error detecting capability in the generated code to detect some of or all the errors that occurred during transmission.
9. **Immunity to noise and Interference:** Another desirable code characteristic is a code that is immune to noise and other interferences.
10. **Cost of Implementation:** It is desirable to keep the encoding technique simple enough such that it does not incur high cost of implementation. A complex scheme is more costly to implement than a simple one.

3.7.2 Line Coding Schemes

- We can divide line coding schemes into three basic categories as shown in Fig. 3.14.

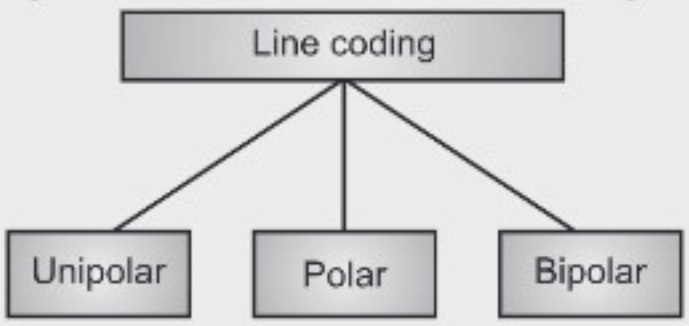


Fig. 3.14: Line Coding Schemes

3.7.2.1 Unipolar Schemes (S-18, 19)

- In unipolar, all the signal levels are on one side of the time axis, either above or below.

(i) NRZ (Non-Return -to-Zero):

- A unipolar scheme was designed as a non-return-to-zero scheme in which positive voltage defines bit 1 and zero voltage defines bit 0.
- In NRZ, signal does not return to zero at the middle of the bit.

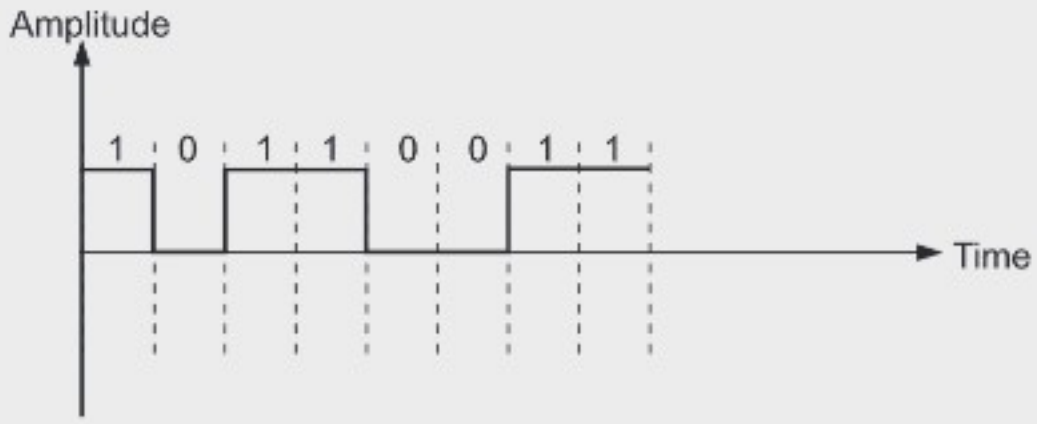


Fig. 3.15: Unipolar NRZ

- In this encoding approach, the bit rate is the same as data rate.

Drawbacks of Unipolar Scheme: (S-18)

(a) Unfortunately, the DC component is present in the encoded signal and there is loss of synchronization for long sequences of 0's and 1's.
(b) It is simple but obsolete.
(c) Unipolar scheme is costly than polar, this scheme is not used in data communications today

3.7.2.2 Polar Schemes

- In polar schemes, the voltages are on both sides of the time axis. It uses two voltage levels – one positive and the other one negative.
- Four different encoding schemes shown in Fig. 3.16 under this category discussed below:

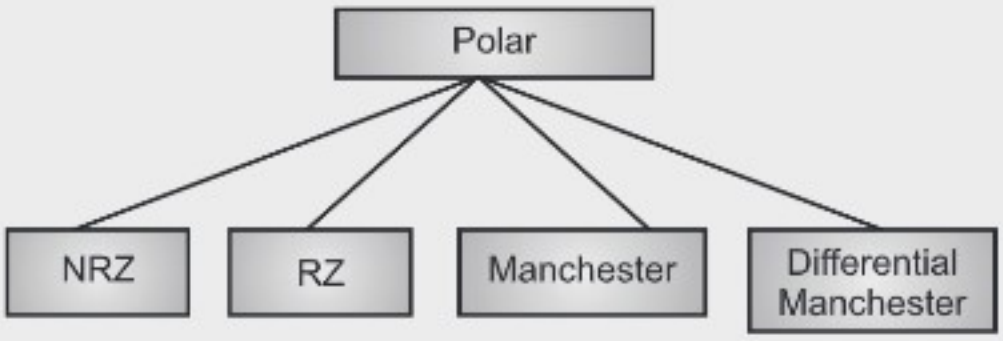


Fig. 3.16: Encoding Schemes under Polar Category

(i) Non-Return-to-Zero (NRZ):

- Polar NRZ is the most common and easiest way to transmit digital signals. It uses two different voltage levels for the two binary digits.

- Usually a negative voltage is used to represent one binary value and a positive voltage to represent the other.
- The data is encoded as the presence or absence of a signal transition at the beginning of the bit time.
- In NRZ encoding, the signal level remains the same throughout the bit-period. Two versions of polar NRZ are NRZ – L and NRZ – I as shown in Fig. 3.17.

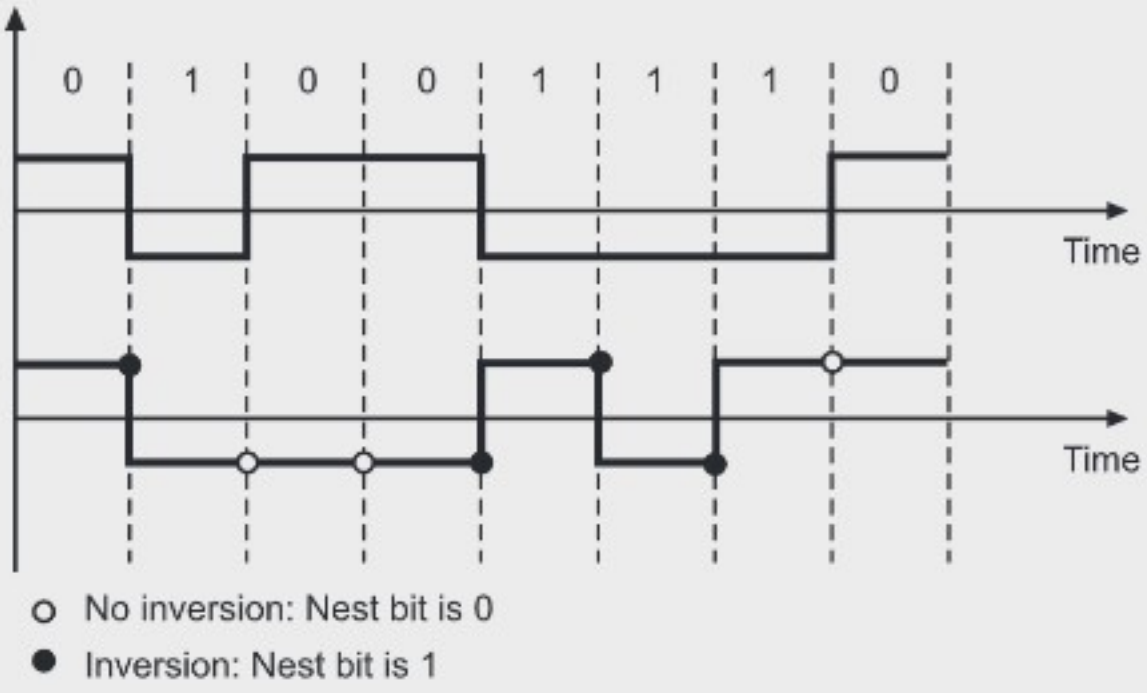


Fig. 3.17: Polar NRZ-L and NRZ-I

- In **NRZ – L,** (L stands for level). The level of the voltage determines the value of the bit. Positive voltage defines 0 bit and negative voltage shows 1 bit.
- In **NRZ – I,** (I stands for invert). The change or lack of change in the level of the voltage determines the value of the bit. If there is no change, the bit is 0, if there is change, the bit is 1.

Advantages of NRZ Coding:

(a) Detecting a transition in presence of noise is more reliable than to compare a value to a threshold.

(b) NRZ codes are easy to engineer and it makes efficient use of bandwidth.

Disadvantages of NRZ Coding:

(a) Baseline wandering is a problem for both methods, it is twice in NRZ-L. If there is a long sequence of 0s or 1s in NRZ-L, the average signal power becomes skewed. The receiver might have difficulty in identifying the bit value. In NRZ-I, this problem occurs only for long sequences of 0s.

(b) The synchronization problem (sender and receiver clocks are not synchronized) also exists in both schemes. Long sequences of 0s can cause a problem in both schemes; a long sequence of 1s affects only NRZ-L.

(c) Another problem with NRZ-L occurs when there is a sudden change of polarity in the system.

(d) NRZ-L and NRZ-I both have a DC component problem.

(ii) Return to Zero (RZ):

- The main problem with NRZ encoding occurs when the sender and receiver clocks are not synchronized. The receiver does not know when one bit has ended and the next bit starting.
- One solution is the return-to-zero (RZ) scheme, which uses three values: positive, negative and zero. In RZ, the signal changes not between bits but during the bit.
- From Fig. 3.18, we see that the signal goes to 0 in the middle of each bit. It remains there until the beginning of the next bit.

Advantages of RZ:

(a) Three levels

(b) Bit rate is double than that of data rate

(c) No dc component

(d) Good synchronization

Disadvantages of RZ:

1. It requires greater bandwidth.
2. Complexity is more since it uses three voltage levels.

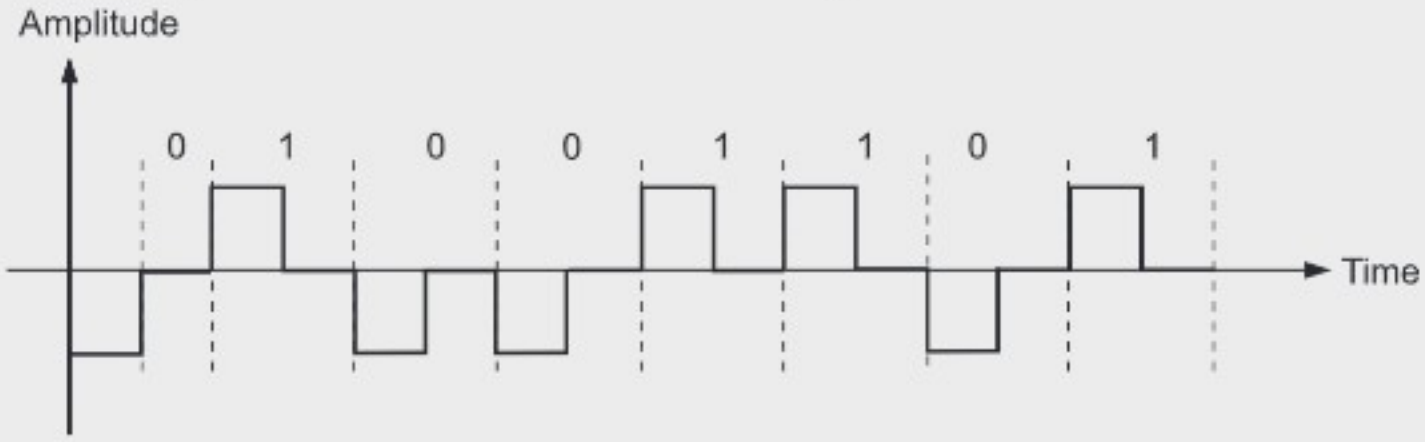


Fig. 3.18: Polar RZ Scheme

(iii) Biphase: Manchester and Differential Manchester:

- To overcome the limitations of NRZ encoding, biphase encoding techniques can be adopted. Manchester and differential Manchester Coding are the two common biphase techniques in use.

A. Manchester: It combines the idea of RZ and NRZ-L. In Manchester encoding, the duration of the bit is divided into two halves. The voltage remains at one level during the first half and moves to the other level in the second half. In Manchester coding the mid-bit transition serves as a clocking mechanism and also as data. There is a transition at the middle of each bit period. A binary 1 corresponds to a low-to-high transition and a binary 0 to a high-to-low transition in the middle.

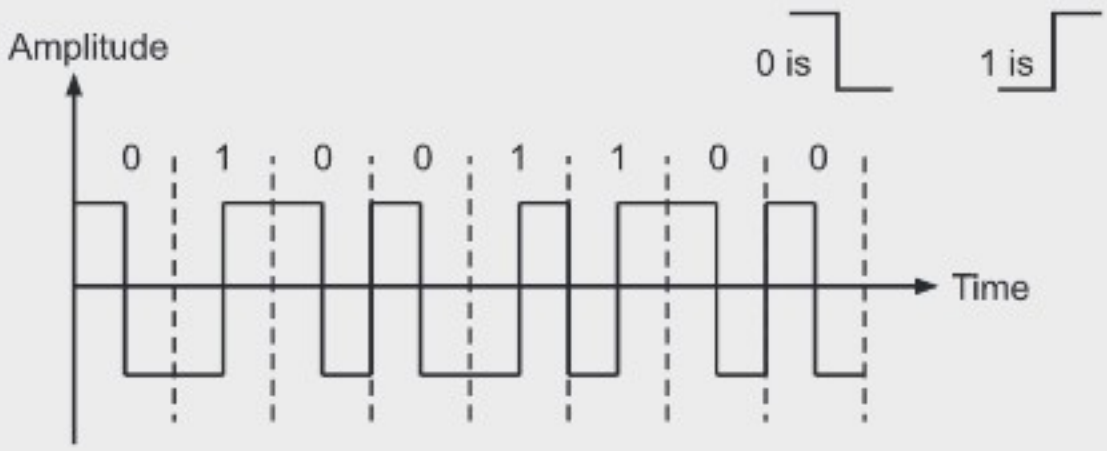


Fig. 3.19: Manchester Encoding

B. Differential Manchester: It combines the idea of RZ and NRZ-I. There is always a transition at the middle of the bit, but the bit values are determined at the beginning of the bit. If the next bit is 0, there is a transition, if the next bit is 1, there is none. Thus in Differential Manchester, inversion in the middle of each bit is used for synchronization.

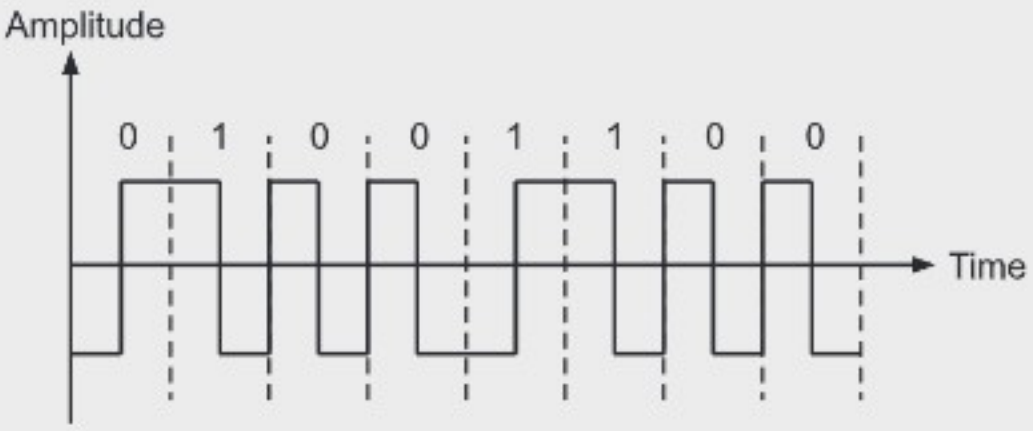


Fig. 3.20: Differential Manchester

Advantages of Biphase:

(a) Two levels.

(b) No DC component and baseline wandering.

(c) Good synchronization.

Disadvantage of Biphase:

(a) The bandwidth required for biphase techniques are greater than that of NRZ techniques. Higher bandwidth is due to doubling of bit rate with respect to data rate.

3.7.2.3 Bipolar Encoding

- It has two types i.e. Bipolar AMI and Bipolar Pseudoternary.
- Bipolar AMI uses three voltage levels. Unlike RZ, the zero level is used to represent a 0 and a binary 1's are represented by alternating positive and negative voltages, as shown in Fig 3.21.

- Bipolar Pseudoternary: This encoding scheme is the same as AMI, but alternating positive and negative pulses occur for binary 0 instead of binary 1.

Advantages of Bipolar:

(a) Three levels.
(b) No DC component.
(c) Loss of synchronization for long sequences of 0's.
(d) Lesser bandwidth.

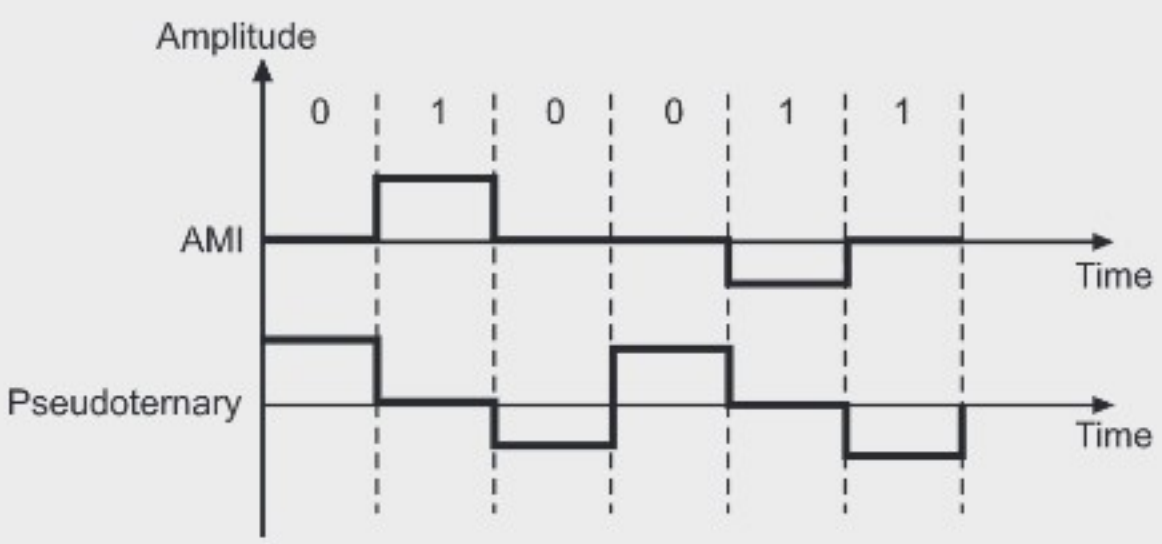


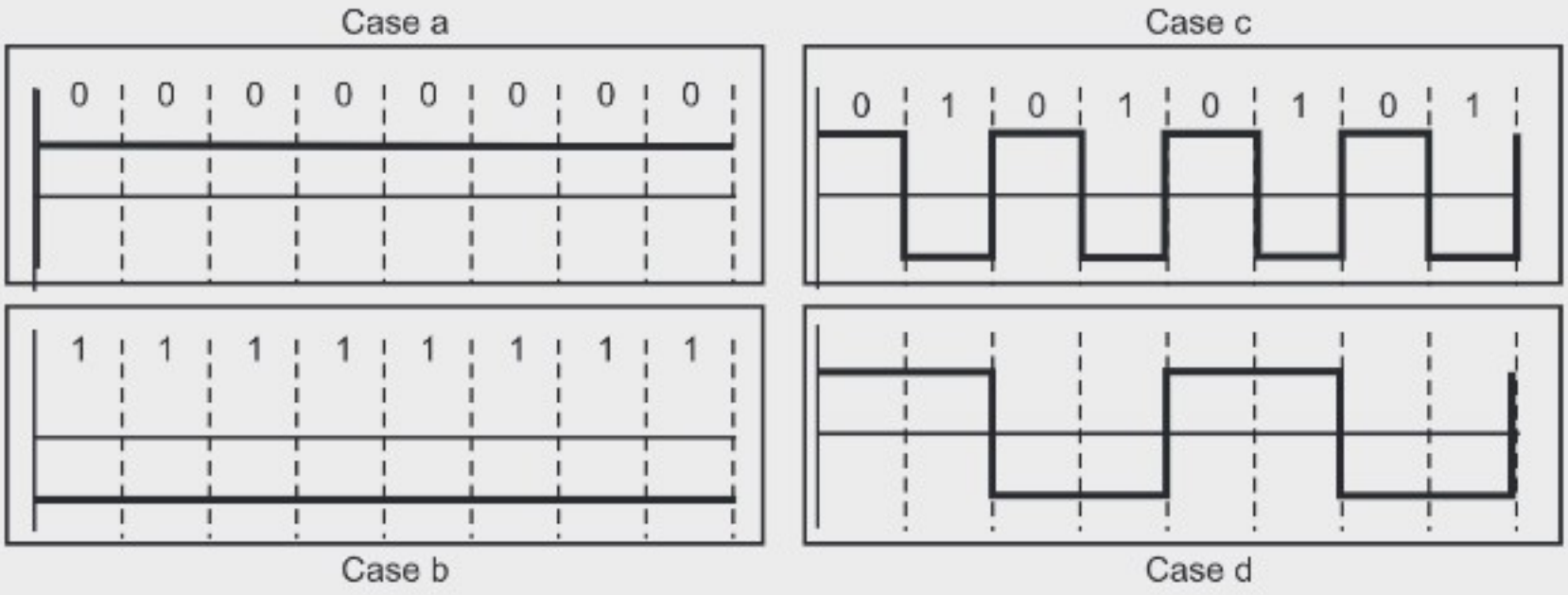
Fig. 3.21: Bipolar AMI and Pseudoternary

Example 13: Draw Graph for NRZ-L, NRZ-I, Manchester and Differential Manchester coding for the following data: **(W-18, S-18)**

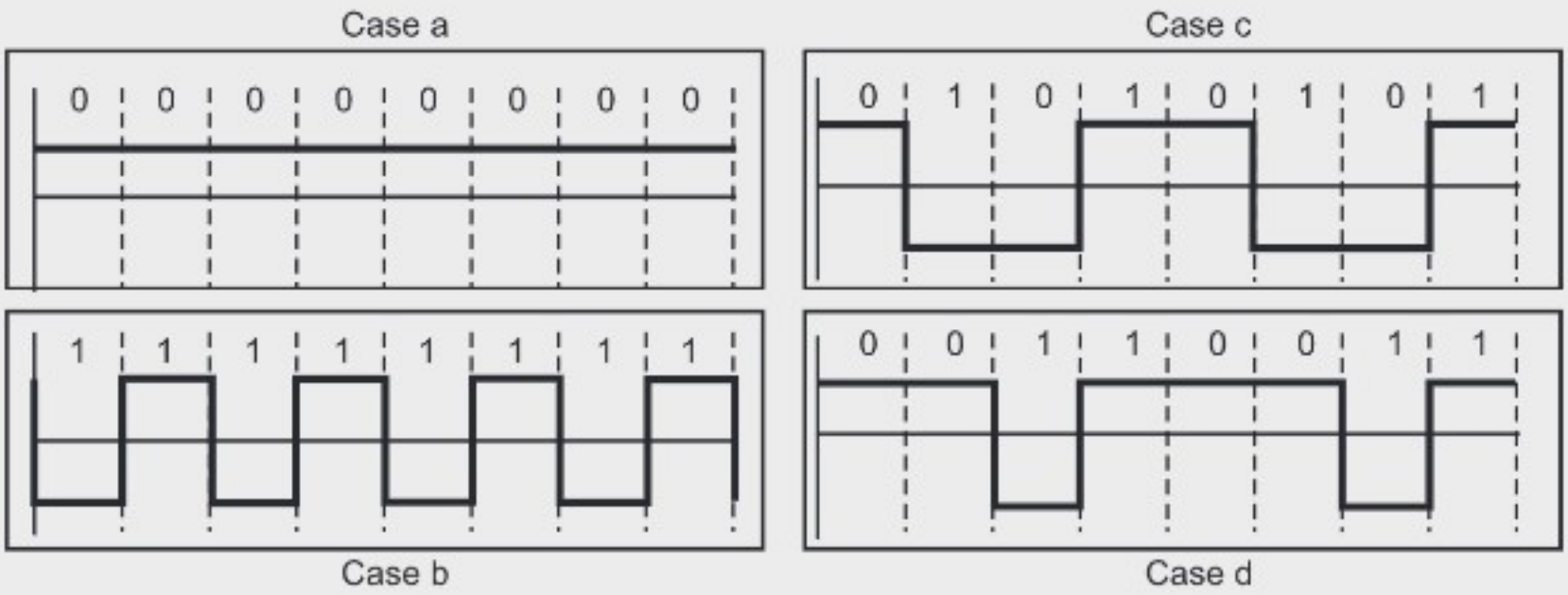
1. 00000000
2. 11111111
3. 01010101
4. 00110011

Solution:

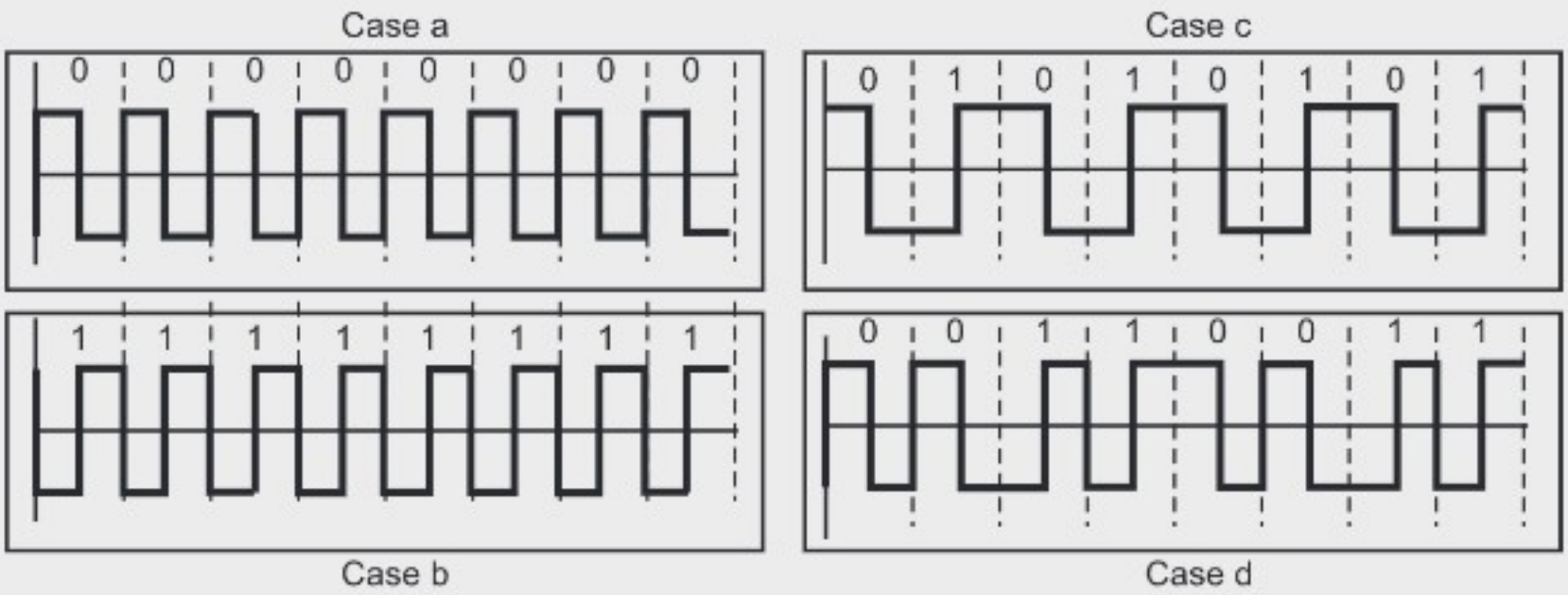
NRZ-L Encoding Scheme:



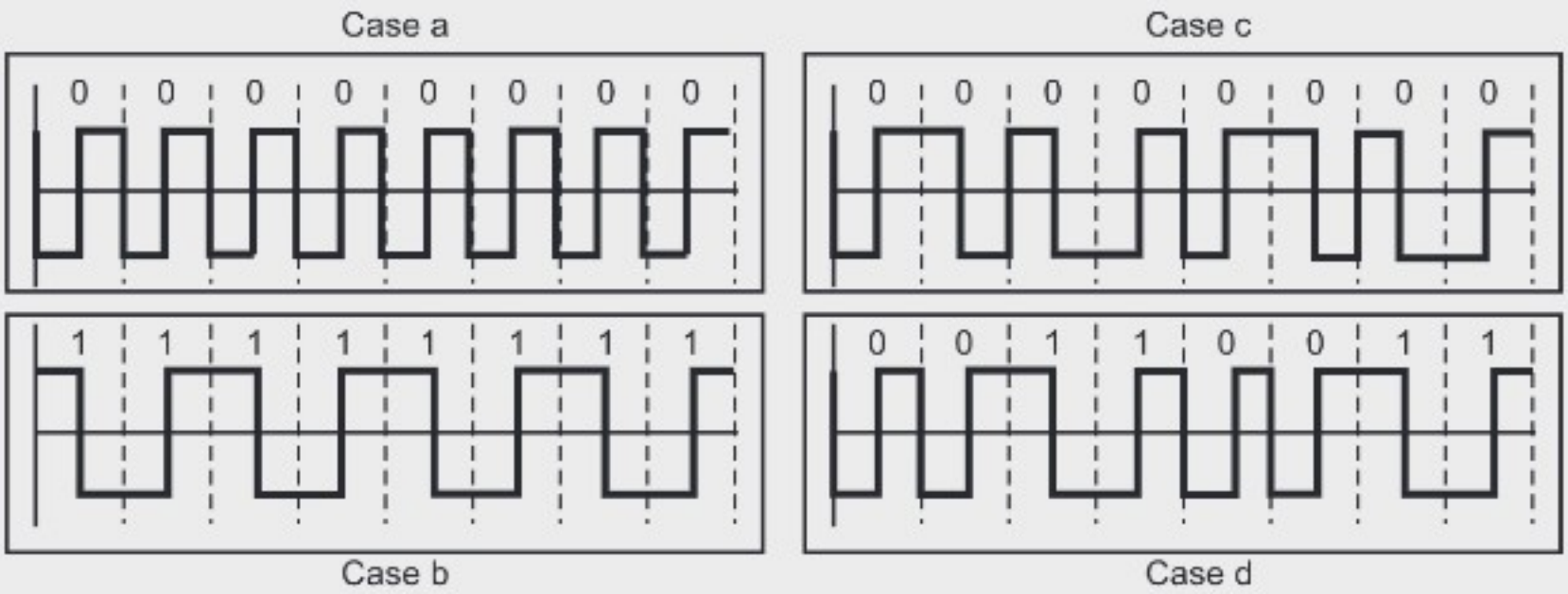
NRZ-I Encoding Scheme:



Manchester Encoding Scheme:



Differential Manchester Encoding Scheme:



3.8 TRANSMISSION MODES (S-18, 19)

- The transmission of binary data across a link can be done in either parallel or serial mode as shown in Fig. 3.22.
- In parallel mode, multiple bits are sent with each clock tick. In serial mode, one bit is sent with each clock tick.
- In parallel transmission, there is only one method to send data.
- In serial transmission, there are three methods of sending data i.e. asynchronous, synchronous and isochronous.

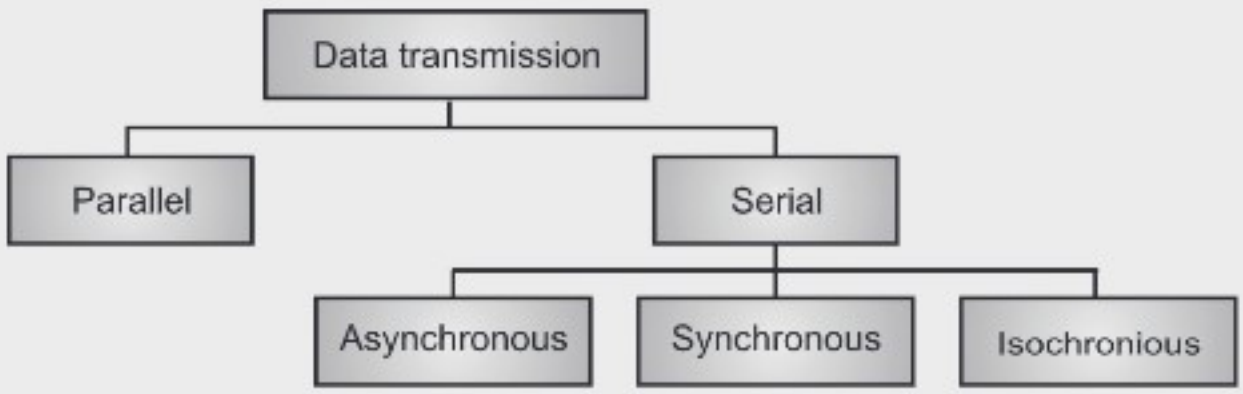


Fig. 3.22: Data Transmission Modes

3.8.1 Parallel Transmission

- Binary data, consisting of 1s and 0s, may be organized into groups of n bits each. Computers produce and consume data in groups of bits.
- By grouping, we can send n data bits at a time instead of 1 bit. This is called parallel transmission.
- In parallel transmission, if we want to send 8 bits, we require 8 wires, one for each bit. The advantage of parallel transmission is speed.
- The main disadvantage is cost. Since parallel transmission uses n communication lines, it is expensive, so it is used for short distances.

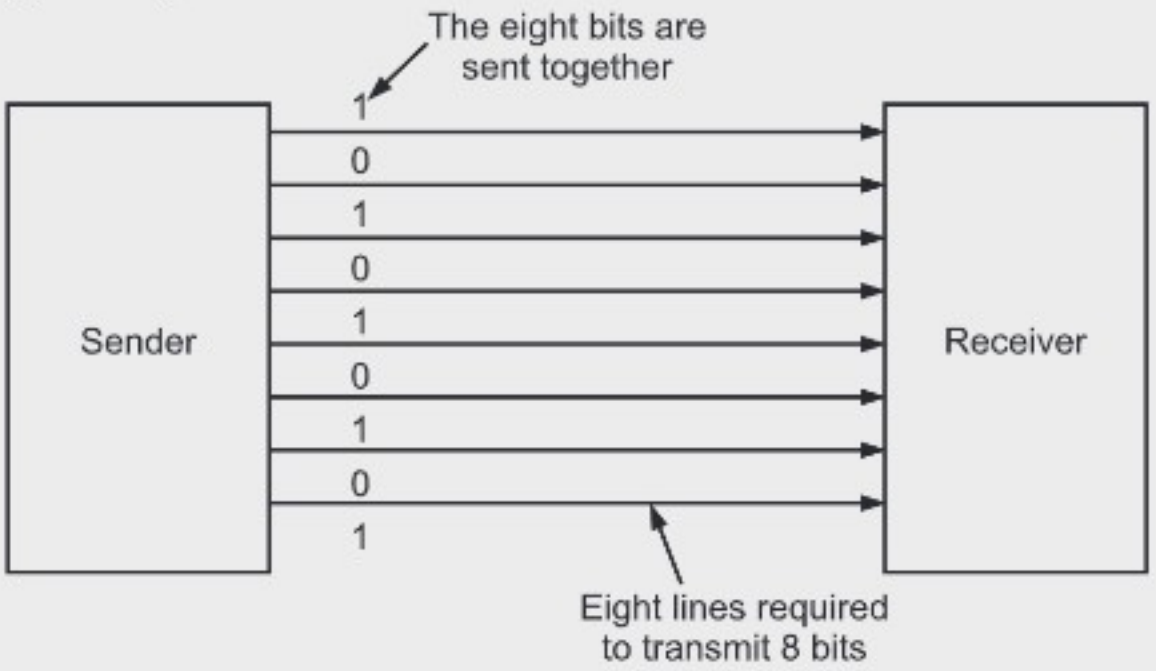


Fig. 3.23: Parallel Transmission

3.8.2 Serial Transmission

- In serial transmission, one bit follows another, so we need only one communication channel rather than n to transmit data between two communicating devices shown in Fig. 3.24.
- Since, communication within devices is parallel, it needs parallel-to-serial and serial-to-parallel conversion at both ends.
- Serial mode of communication widely used because of the following advantages:
  1. **Reduced cost of cabling:** Lesser number of wires is required as compared to parallel connection.
  2. **Reduced cross talk:** Lesser number of wires result in reduced crosstalk availability of suitable communication media.
  3. **Inherent device characteristics:** Many devices are inherently serial in nature portable devices like PDAs, etc use serial communication to reduce the size of the connector
- However, it is slower than parallel mode of communication.

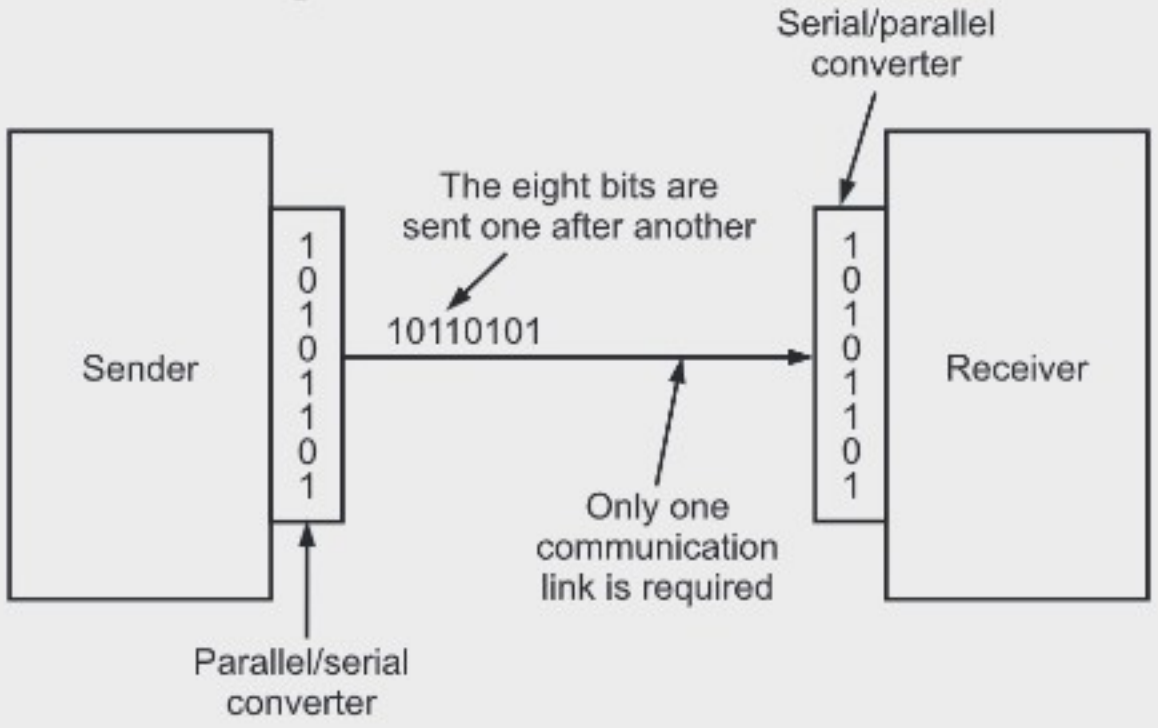


Fig. 3.24: Serial Transmission

- Serial transmission occurs in one of three ways i.e., Asynchronous, Synchronous, and Isochronous.

3.8.2.1 Asynchronous Transmission

- In asynchronous transmission, timing of a signal is unimportant. Instead, information is received and translated by agreed upon patterns. Patterns are based on grouping the bit stream into bytes. Generally every group is of 8 bits. Every group is handled independently, relaying it to the link whenever ready, without regard to a timer.

- To alert the receiver to the arrival of a new group, an extra bit is added to the beginning of each byte, usually 0, called the start bit. To know the receiver byte is finished, additional 1 bit is appended at the end of the byte. This bit is called a stop bit.
- The start and stop bits and the gap alert the receiver about the beginning and end of each byte.
- This mechanism is called asynchronous because, at the byte level, the sender and receiver do not have to be synchronized. But within each byte, the receiver must still be synchronized with the incoming bit stream. That is, some synchronization is required, but only for the duration of a single byte. The receiving device synchronized at the onset of each new byte.
- Fig. 3.25 shows an illustration of asynchronous transmission.

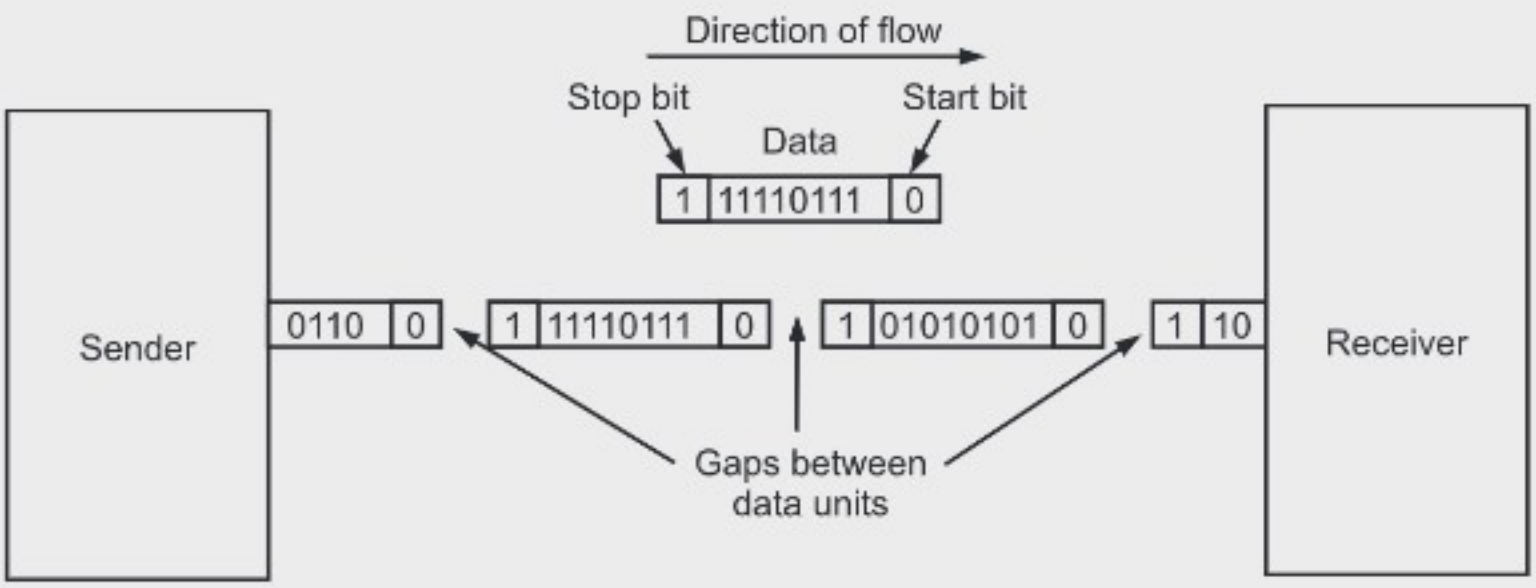


Fig. 3.25: Asynchronous Transmission

3.8.2.2 Synchronous Transmission

- In synchronous transmission, the bit stream is combined into longer "frames," which may contain multiple bytes.
- We send bits one after another without start or stop bits or gaps as shown in Fig. 3.26.

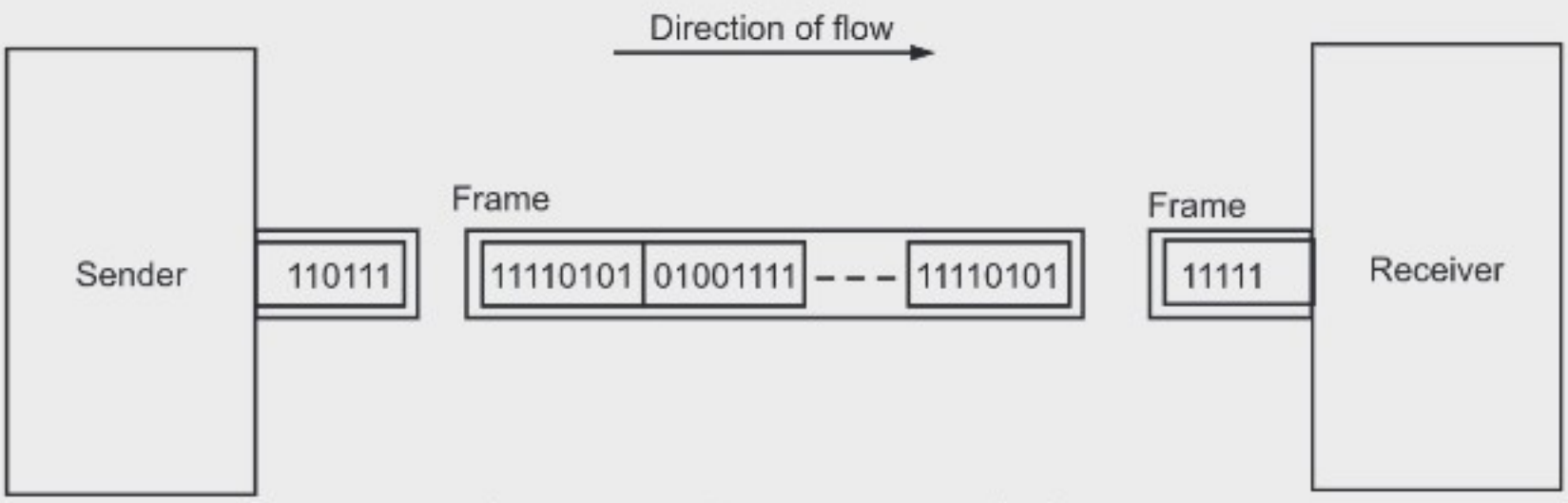


Fig. 3.26: Synchronous Transmission

- It is the responsibility of the receiver to group the bits. The sender puts its data onto the line as one long string. The receiver counts the bits as they arrive and groups them in 8-bit units.
- Without gaps and start and stop bits, there is no built-in mechanism to help the receiving device adjust its bit synchronization midstream. Timing becomes very important, therefore, because the accuracy of the received information is completely dependent on the ability of the receiving device to keep an accurate count of the bits as they come in.
- The advantage of synchronous transmission is speed. It is more useful for high speed applications such as the transmission of data from one computer to another. Although there is no gap between characters in synchronous serial transmission, there may be uneven gaps between frames.

Table 3.2: Comparison between Synchronous and Asynchronous data Transmission.

Sr. No.	Factors	Asynchronous Transmission	Synchronous Transmission
1.	Data sent at one time	Usually 1 byte	Multiple bytes
2.	Start and stop bit	Used	Not used
3.	Gap between data units	Present	Not present
4.	Data transmission speed	Slow	Fast
5.	Cost	Low	High

3.8.2.3 Isochronous Transmission

- Isochronous transmission is designed to provide steady bit flow for multimedia applications.
- In real time audio and video, in which uneven delays between frames are not acceptable, synchronous transmission fails. For frames like TV images, must be viewed at the same rate. For such applications, there should be no delays between frames. Delivering such data at a steady rate is essential because variations in delay known as jitter can disrupt reception.
- For multimedia applications, synchronization between characters is not enough, the entire stream of bits must be synchronized. The isochronous transmission guarantees that the data arrive at a fixed rate.

3.9 MULTIPLEXING FDM AND TDM (S-19)

- In this section, we will discuss different multiplexing and switching techniques.
- 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.
- Switching is a process to forward packets coming in from one port to a port leading towards the destination.
- It has been observed that most of the individual data communicating devices typically require modest data rate. But, communication media usually have much higher bandwidth. As a consequence, two communicating stations do not utilize the full capacity of a data link. Moreover, when many nodes compete to access the network, some efficient techniques for utilizing the data link are very essential.
- When the bandwidth of a medium is greater than individual signals to be transmitted through the channel, a medium can be shared by more than one channel of signals. The process of making the most effective use of the available channel capacity is called Multiplexing.
- Multiplexing is the set of techniques that allows the simultaneous transmission of multiple signals across a single data link. Bandwidth utilization is the wise use of available bandwidth to achieve specific goals.
- In a multiplexed system, n lines share the bandwidth of one link. Fig. 3.27 shows the basic format of the multiplexed system.
- A multiplexer (MUX) combines all i/p lines into a single stream (many-to-one). At receiving end, the stream is fed to a demultiplexer (DEMUX), which separates the stream back into its component transmission (one-to-many) and directs them to their corresponding lines.

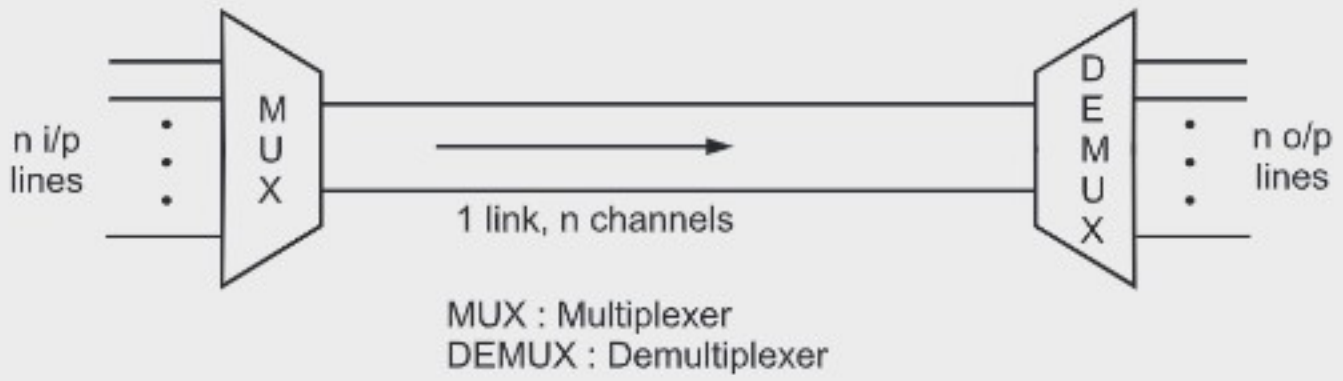


Fig. 3.27: Basic Concept of Multiplexing

- There are three basic multiplexing techniques as shown in Fig. 3.28 i.e.,
  1. Frequency Division Multiplexing (FDM).
  2. Wavelength Division Multiplexing (WDM).
  3. Time Division Multiplexing (TDM).

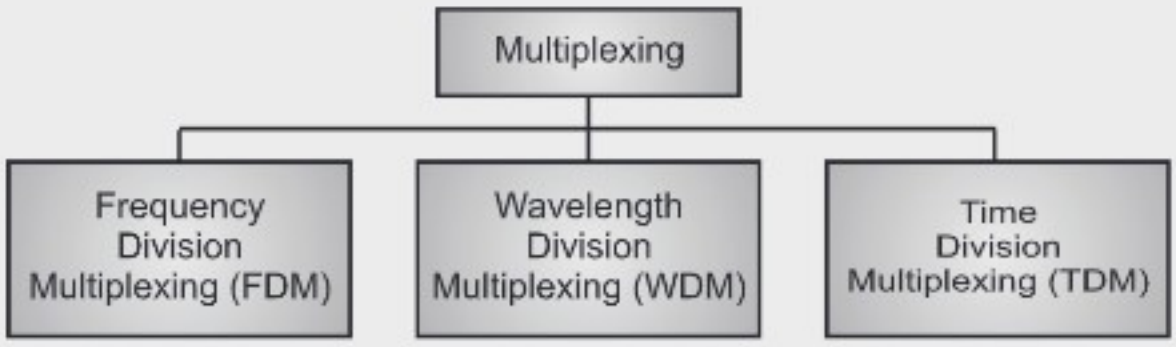


Fig. 3.28: Categories of Multiplexing

3.9.1 FDM (S-19)

- Frequency Division Multiplexing (FDM) is an analog technique.
- It divides the spectrum into frequency bands, with each user having exclusive possession of some band in which to send their signal.
- In FDM, signals generated by each sending device modulate different carrier frequencies. All the modulated signals are combined in a linear summing circuit to form a composite signal for transmission. The carriers used to modulate the individual message signals are called sub-carriers.
- At the receiving end the signal is applied to a bank of band-pass filters, which separates individual frequency channels. The band pass filter outputs are then demodulated and distributed to different output channels.
- If the channels are very close to one another, it leads to inter-channel crosstalk. Channels must be separated by strips of unused bandwidth to prevent inter-channel crosstalk. These unused channels between each successive channel are known as guard bands. Guard bands keeps the channels well separated
- It is most popular and is used extensively in radio and TV transmission.

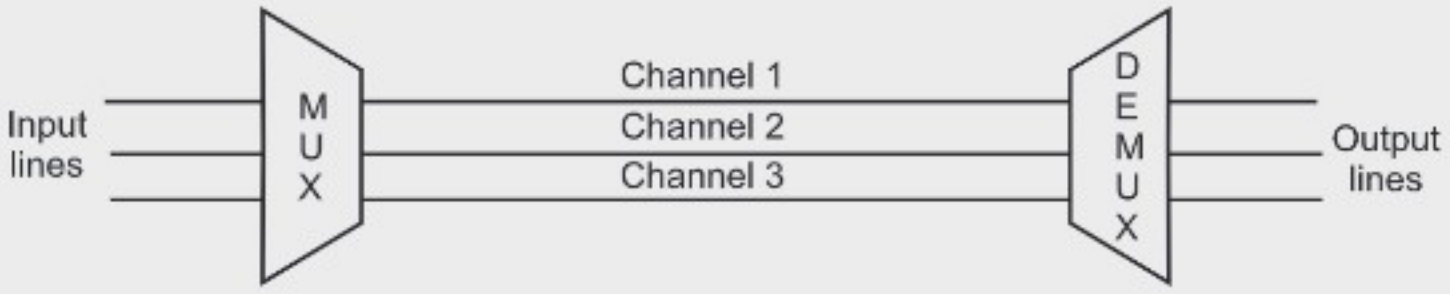


Fig. 3.29: Frequency Division Multiplexing (FDM)

3.9.2 WDM

- Wavelength Division Multiplexing (WDM) is designed to use the high data rate capacity of fiber optic cable.
- Using a fiber optic cable for one single line wastes the available bandwidth.
- WDM is complex and conceptually the same as FDM.

- Multiplexing allows us to combine several lines into one. Very narrow bands of light signal from different sources are combined to make a wider band of light. At the receiver the signals are separated with the help of a demultiplexer.

3.9.3 TDM (S-19)

- In TDM the users take turns (in a round-robin fashion),each one periodically getting the entire bandwidth for a little burst of time
- Time-Division Multiplexing (TDM) is a digital process that allows several connections to share the bandwidth of a link as shown Fig. 3.30. In FDM, time is shared. In TDM, the same link is used.
- In the Fig. 3.30, portions of signals 1, 2, 3, and 4 occupy the link sequentially.

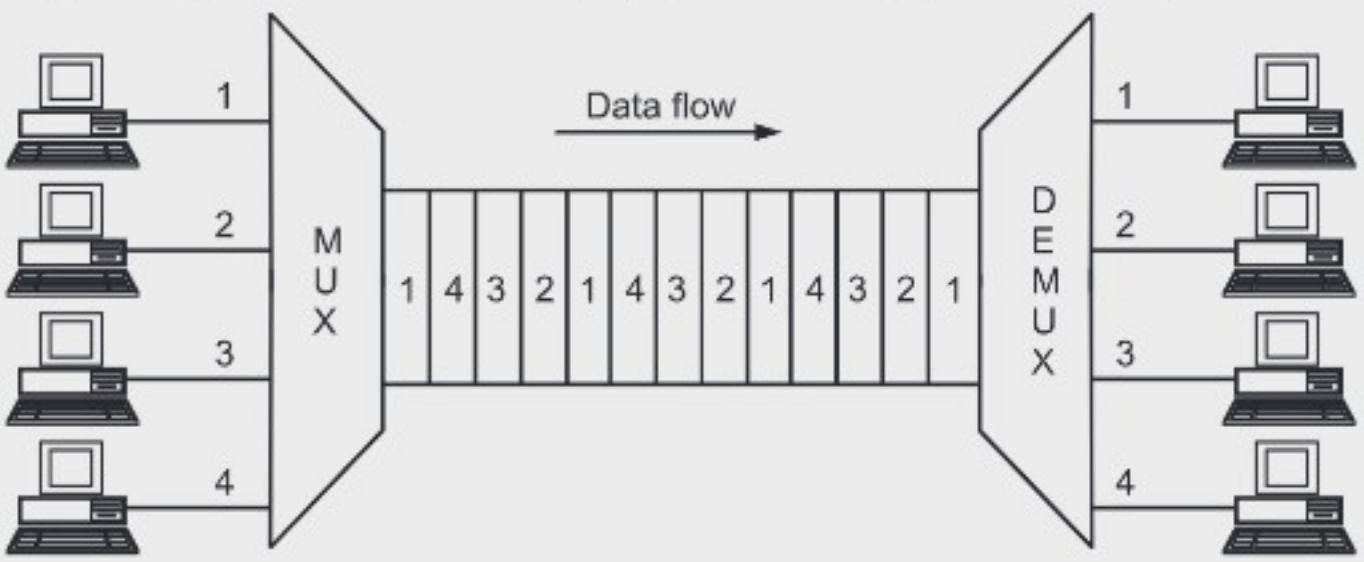


Fig. 3.30: Time Division Multiplexing (TDM)

- Bits from each input stream are taken in a fixed time slot and output to the aggregate stream. This stream runs at the sum rate of the individual streams. For this to work, the streams must be synchronized in time. Small intervals of guard time analogous to a frequency guard band may be added to accommodate small timing variations.
- TDM can be divided into synchronous TDM and statistical TDM.
  1. **Synchronous TDM,** which is commonly used for multiplexing digitized voice streams. The users take turns using the entire channel for a short burst of time. Each time slot is pre-assigned to a fixed source. The time slots are transmitted irrespective of whether the sources have any data to send or not.
  2. **Statistical TDM** which is also called asynchronous TDM, which simply improves on the efficiency of synchronous TDM. It dynamically allocates the time slots on demand to separate input channels, thus saving the channel capacity.
- TDM is used widely as part of the telephone and cellular networks.

Table 3.3: The following table shows the difference between FDM and TDM

Sr. No.	TDM	FDM
1.	TDM is a technique for transmitting several messages on one channel by dividing time domain slots. One slot for each message.	In FDM technique to transmit several messages on one channel, message signals are distributed in frequency spectrum such that they do not overlap.
2.	In TDM perfect synchronization between transmitter and receiver is required.	In FDM synchronization between transmitter and receiver is not required.
3.	It is usually preferred for digital signal transmission.	It is usually preferred for analog signal transmission.
4.	TDM does not require very complex circuitry.	It requires complex circuitry at transmitter and receiver.
5.	It requires a commutator at the transmitting end and a distributor, working in perfect synchronization with the commutator at the receiving end.	FDM requires modulators, filters and demodulators.
6.	Crosstalk problem is not severe in TDM.	FDM suffers from crosstalk problem due to imperfect bandpass filter.
7.	TDM is used widely as part of the telephone and cellular networks.	FDM is used extensively in radio and TV transmission.

3.10 SWITCHING TECHNIQUES (W-18)

- A network is a set of connected multiple devices, whenever multiple devices are there, we have the problem of how to connect them to make one-to-one communication possible. If a network is a LAN, we can have point to point or broadcast links. But for WAN, such topologies are not possible.
- A better solution is switching. A switched network consists of a series of interlinked nodes, called switches.
- Switches are devices capable of creating temporary connection between two or more devices linked to the switch.
- In switched networks, some of these nodes are connected to the end systems (computers or telephones). Others are used only for routing.

- Fig. 3.31 shows switched network.

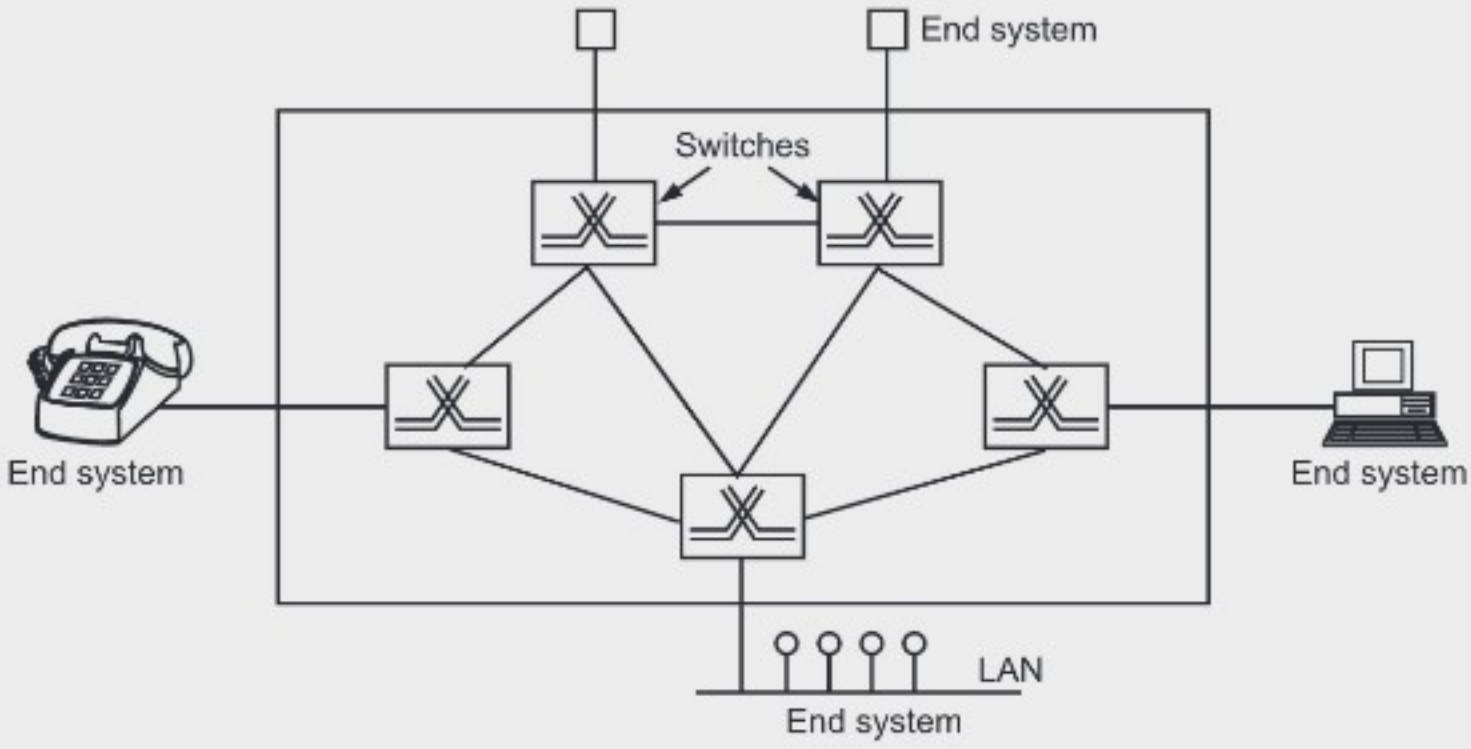


Fig. 3.31: Switched Network

Key Features of a Switched Communication Network:

1. Network topology is not regular.
2. Uses FDM or TDM for node-to-node communication.
3. There exist multiple paths between a source-destination pair for better network reliability.
4. The switching nodes are not concerned with the contents of data.
5. Their purpose is to provide a switching facility that will move data from node to node until they reach the destination.

- The switching performed by different nodes can be categorized into the following three types i.e., Circuit Switching, Packet Switching and Message Switching.
- Circuit and packet switching are commonly used today. Message switching has been phased out in general communications.

3.10.1 Circuit Switching

- Circuit switching is commonly used technique in telephony, where the caller sends a special message with the address of the callee (i.e. by dialing a number) to state its destination.
- Fig. 3.32 shows the concept of circuit switching. In Fig. 3.32, six different rectangles are shown. Each rectangle represents a carrier switching office (end office, toll office etc). As an example, we have shown every office has three incoming and three outgoing lines.

- When a call passes through a switching office, a physical conceptual temporary connection is established between the line on which the call came in and one of the output lines, as shown by dotted lines.
- Once a call has been set up, a dedicated path between both ends exists and will continue to exist until the call is finished.

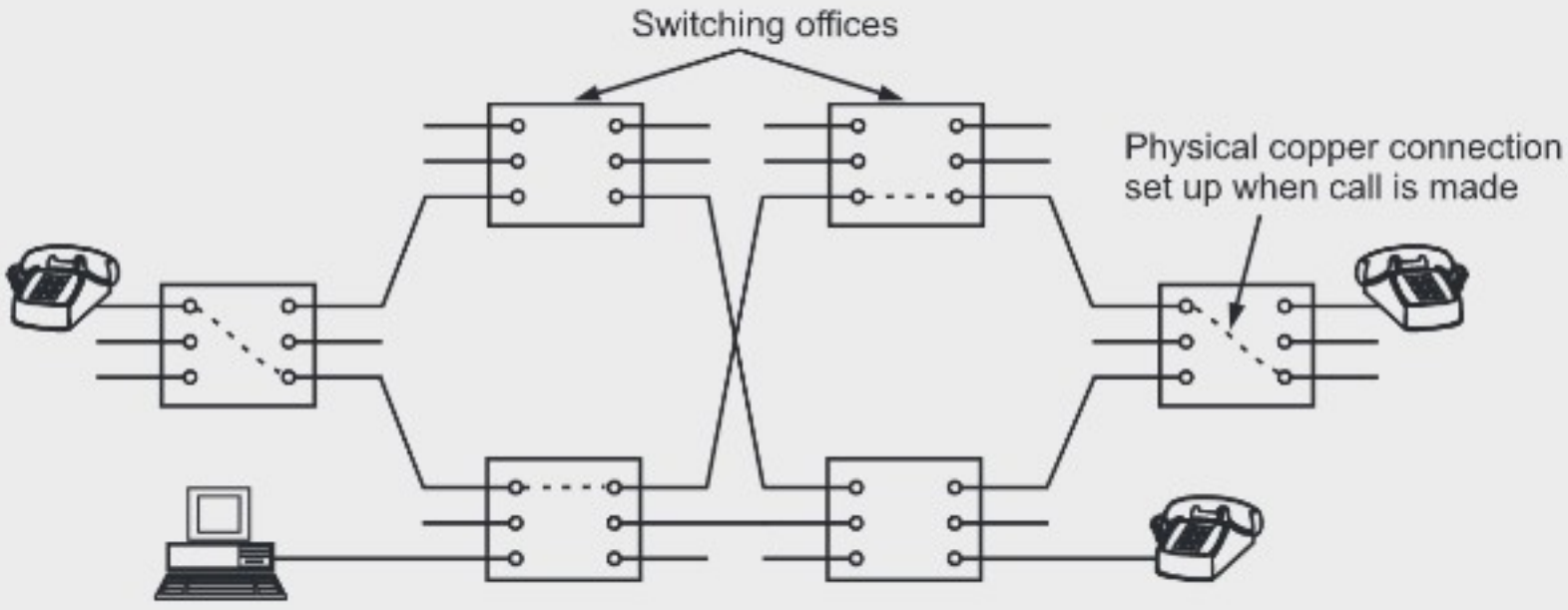


Fig. 3.32: Circuit Switching

- Communication via circuit switching implies that there is a dedicated communication path between the two stations. The path is connected through a sequence of links between network nodes. It involves the following three distinct steps:

1. **Circuit Establishment:**
   - To establish an end-to-end connection before any transfer of data.
   - Some segments of the circuit may be a dedicated link, while some other segments may be shared.
2. **Data Transfer:**
   - Transfer data is from the source to the destination.
   - The data may be analog or digital, depending on the nature of the network.
   - The connection is generally full-duplex.
3. **Circuit Disconnect**:
   - Terminate connection at the end of data transfer.
   - Signals must be propagated to deallocate the dedicated resources.

- Thus, the actual physical electrical path or circuit between the source and destination host must be established before the message is transmitted. This connection, once established, remains exclusive and continuous for the complete duration of information exchange and the circuit becomes disconnected only when the source wants to do so.

Advantages:

1. **Fixed bandwidth and guaranteed capacity:** That means there is an end-to-end link and since end-to-end link is there the bandwidth is fixed and it does not change. After the establishment of the link, both the ends know what is the possible transfer rate and there is no possibility of congestion.
2. **Low variance in end-to-end delay:** There is low variance in end-to-end delay, there is a constant delay. This delay is essentially the propagation time so there is no other delay involved in this communication.

Disadvantages:

1. The circuit establishment and circuit disconnect introduces extra overhead and delay
2. Constant data rate from source to destination
3. Channel capacity is dedicated for the duration of the connection even if no data is transferred. That means after circuit establishment if data is not transferred obviously the bandwidth is wasted.
4. Inefficient for bursty traffic. A typical user host data connection the line utilization is very poor.
5. Whenever the user is not using the bandwidth, that bandwidth others cannot use even if it is free of traffic.

3.10.2 Message Switching (S-19)

- Another switching technique is message switching. In this switching method, a different strategy is used, where instead of establishing a dedicated physical line between the sender and the receiver, the message is sent to the nearest directly connected switching node as shown in Fig. 3.33.
- This node stores the message, checks for errors, selects the best available route and forwards the message to the next intermediate node.

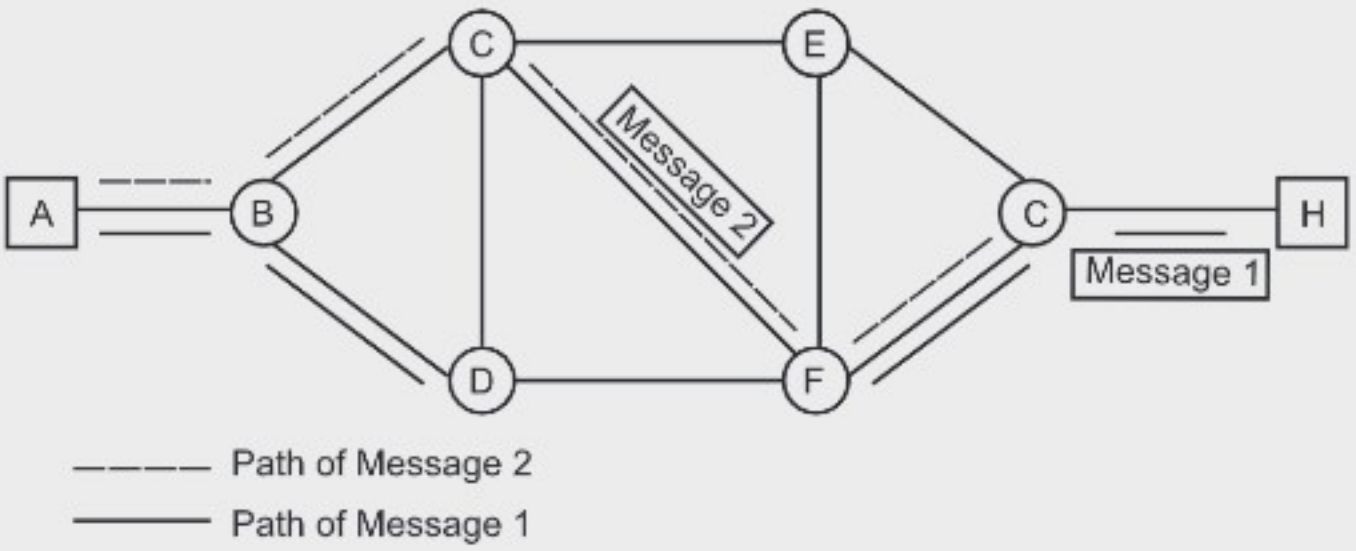


Fig. 3.33: Concept of Message Switching

- The line becomes free again for other messages, while the process is being continued in some other nodes. Due to the mode of action, this method is also known as **store-and-forward technology** where the message hops from node to node to its final destination. Each node stores the full message, checks for errors and forwards it.

Advantages:

1. In message switching, no circuit setup is required in advance.
2. Line efficiency is greater (sharing of links).
3. Data rate conversion is possible.
4. Message priorities can be used, to satisfy the requirements, if any.

Disadvantages:

1. Every switch in the transit path needs enough storage to accommodate the entire message.
2. Because of store-and-forward technique and waits included until resources are available, message switching is very slow. If there is a lot of traffic on the network, the delay will be very high, reducing throughput.
3. Message switching was not a solution for streaming media and real-time applications.

3.10.3 Packet Switching

- The basic approach is not much different from message switching. It is also based on the same 'store-and-forward' approach.
- However, to overcome the limitations of message switching, messages are divided into subsets of equal length called packets.
- Packet switching approach was developed for long-distance data communication (1970) and it has evolved over time.
- In the packet switching approach, data is transmitted in short packets (few Kbytes). A long message is broken up into a series of packets as shown in Fig. 3.34.

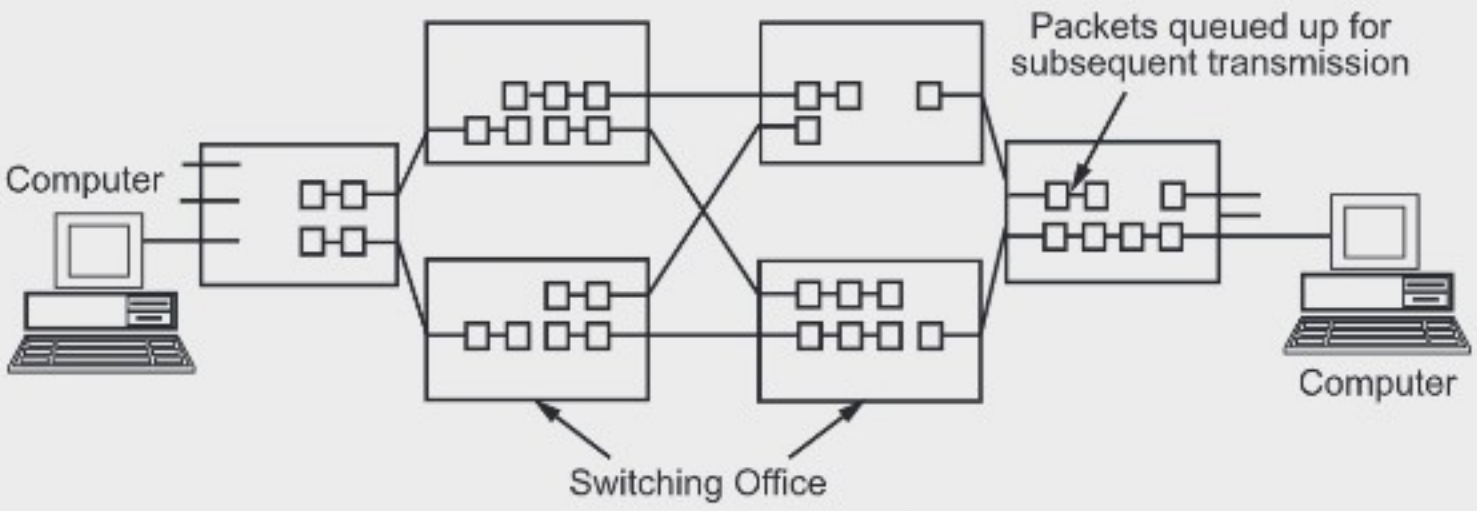


Fig. 3.34: Packet Switching

- Every packet contains some control information in its header, which is required for routing and other purposes.

- Main difference between Packet switching and Circuit Switching is that the communication lines are not dedicated to passing messages from the source to the destination.
- In Packet Switching, different packets can pass through different routes, and when there is a "dead time" in the communication between the source and the destination, the lines can be used by other sources.
- Packet switching networks are well suited for handling interactive traffic, by making sure that no user holds the transmission line for a long time.
- In cases where traffic fees are charged, for example in cellular communication, packet switching is characterized by a fee per unit of information transmitted.

Advantages:

1. No circuit set up required in advance.
2. No Bandwidth is reserved.
3. Used for performing data rate conversion.
4. More fault tolerant.

Disadvantages:

1. In packet switching, different packets can follow different paths, so they may arrive out of order.
2. If a node crashes momentarily, all of its queued packets are lost

- Fig. 3.35 shows timing events of above three switching techniques.

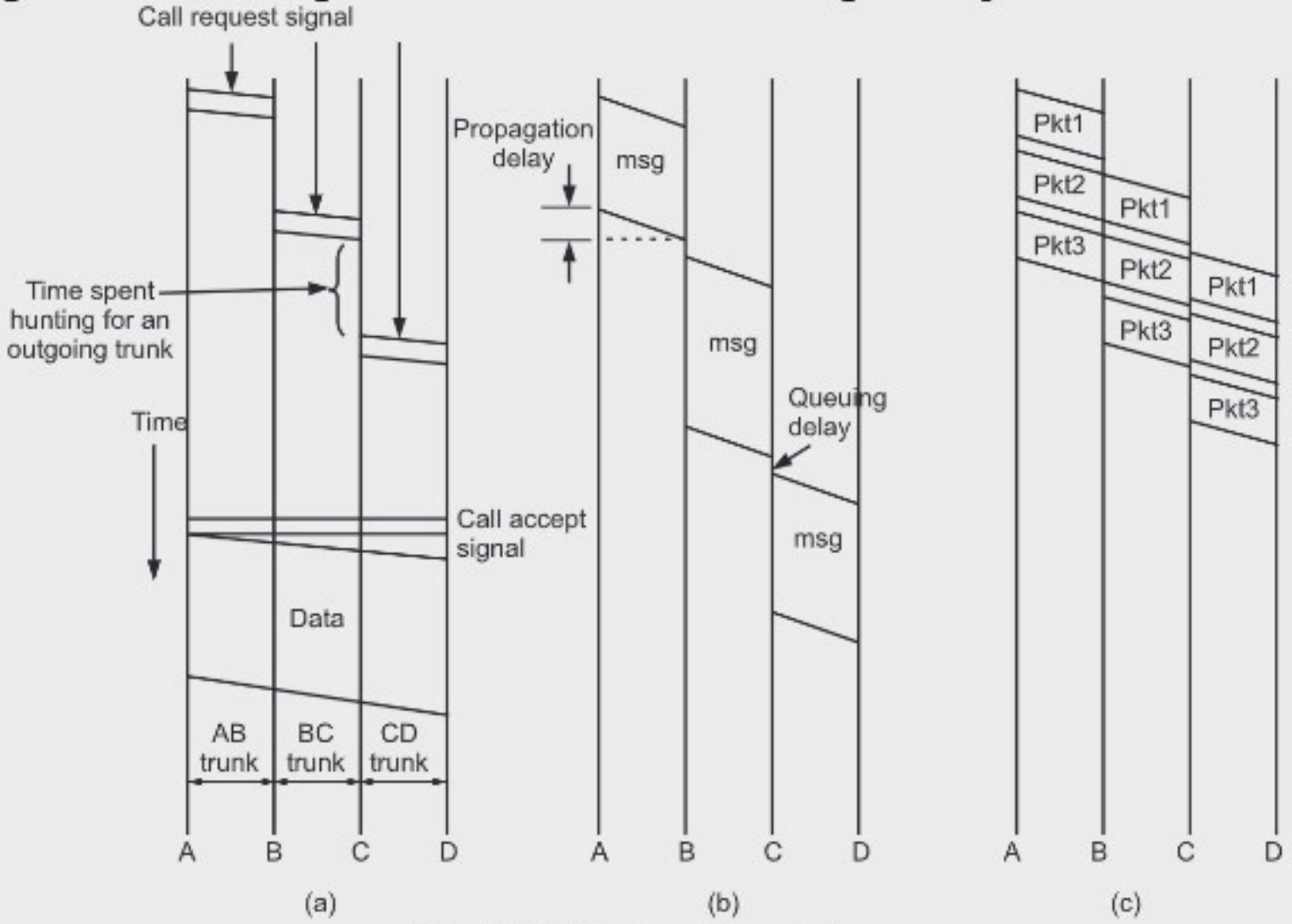


Fig. 3.35: Timing of events in
(a) Circuit Switching (b) Message Switching (c) Packet Switching

3.10.4 Comparison of Circuit, Packet and Message Switching

- Following points compare circuits, packet and message switching:

1. Circuit switching requires advance setup. Bandwidth is reserved first and then data is transmitted. Packet switching does not require any advance setup. The first packet can just be sent as soon as it is available.
2. In circuit switching, all packets follow the same path, they arrive in order. With packet switching, there is no path, so different packets can follow different paths, they may arrive out of order.
3. Packet switching is more fault tolerant than circuit switching.
4. In circuit switching, since bandwidth is reserved, the packet is sent out immediately over the reserved bandwidth. With packet switching, no bandwidth is reserved, so packets may have to wait their turn to be forwarded.
5. In circuit switching, congestion can occur at set-up time only. But in packet switching, congestion can occur at any time.
6. If a circuit has been reserved for a particular user and there is no traffic to send, the bandwidth of that circuit is wasted. It cannot be used for other traffic. Packet switching does not waste bandwidth and thus is more efficient.
7. Packet switching uses store and forward transmission. A packet is accumulated in a router's memory, then sent onto the next router. With circuit switching, the bits just flow through a wire continuously.
8. Circuit switching is completely transparent than packet switching.
9. In circuit switching, the routing decisions have to be made at the time of call setup.

   In packet switching, a routing decision has to be made individually for every packet at each intermediate node.
10. A final difference between circuit and packet switching is the charging algorithm. In circuit switching, charging is based on distance and time. For packet switching, charging is based on volume of traffic.

Comparison Summary:

Table 3.4: Comparison between Circuit and Packet Switching

Parameters	Circuit switched	Packet switched
1. Call setup	Required	Not needed
2. Dedicated physical path	Yes	No
3. Each packet follows the same route	Yes	No
4. Packets arrive in order	Yes	No
5. Is a switch crush fatal	Yes	No
6. Bandwidth available	Fixed	Dynamic

7. Time of possible congestion	At setup time	On every packet
8. Potentially wasted bandwidth	Yes	No
9. Store and forward transmission	No	Yes
10. Transparency	Yes	No
11. Charging	Per minute	Per packet

Summary

- The physical layer is concerned with transmission of raw bits over a communication channel.
- Data refers to information that conveys some meaning based on some mutually agreed up rules or conventions between a sender and a receiver and today it comes in a variety of forms such as text, graphics, audio, video and animation.
- Data can be analog or digital.
- Analog data are continuous values.
- Digital data have discrete states and take discrete values.
- Signal is an electrical, electronic or optical representation of data, which can be sent over a communication medium.
- Signals can be either analog or digital.
- Analog signals can have an infinite number of values in a range.
- Digital signals can have only a limited number of defined values.
- Both analog and digital signals can take one of two forms: periodic and non-periodic.
- In data communication, we commonly use periodic analog signals and non-periodic digital signals.
- Periodic analog signals can be classified as simple or composite.
- A simple periodic analog signal is a sine wave which cannot be decomposed into simpler signals.
- A composite periodic analog signal is composed of multiple sine waves.
- A sine wave can be represented by three parameters: the peak amplitude, the frequency, and the phase.
- Most digital signals are non-periodic and thus, period or frequency is not appropriate. Two new terms, bit interval and bit rate are used to describe digital signals instead of period and frequency respectively.
- The bit interval is the time required to send one single bit.
- The bit rate is the number of bit intervals per second. This means that the bit rate is the number of bits sent in one second, usually expressed in bits per second (bps).
- The bit length is the distance one bit occupies on the transmission medium.

  Bit length = propagation speed × bit duration

- We can transmit a digital signal by using baseband transmission or broadband transmission (using modulation).
- Baseband transmission means sending a digital signal over a channel without changing the digital signal to an analog signal.
- Broadband transmission or modulation means changing the digital signal to an analog signal for transmission.
- When a signal is transmitted over a communication channel, it is subjected to different types of impairments because of imperfect characteristics of the channel.
- The impairment can be broadly categorized into the following three types: attenuation, distortion and noise.
- Attenuation means a loss of energy. When a signal travels through a medium, it loses some of its energy in overcoming the resistance of the medium.
- To show that a signal has lost or gained strength, unit decibel is used.
- Distortion means that the signal changes its form or shape. Distortion can occur in a composite signal made of different frequencies.
- As a signal is transmitted through a channel, undesired signal in the form of noise gets mixed up with the signal, along with the distortion introduced by the transmission media.
- Noise can be categorized into the following four types: Thermal Noise , Induced Noise, Crosstalk and Impulse Noise.
- Data rate depends upon: bandwidth available, level of the signals and quality of the channel.
- Nyquist Bit Rate formula for noiseless channel is,

  Bit rate = $2 \times \text{bandwidth} \times \log_2 L$.
- Shannon introduced a formula, called Shannon capacity, to determine the theoretical highest data rate for noisy channels.

  Capacity = Bandwidth $\times \text{Log}_2 (1 + \text{SNR})$
- Performance of the network depends upon several factors, they are: Bandwidth, Throughput, Latency (delay), Bandwidth delay product and Jitter.
- In networking, we use the term bandwidth in two contexts. Bandwidth in hertz refers to the range of frequencies in a composite signal or the range of frequencies that the channel can pass. Bandwidth in bits per second refers to the speed of bit transmission in a channel or link.
- The throughput is a measure of how fast we can actually send data through a network.
- The latency or delay defines how long it takes for an entire message to completely arrive at the destination from the time the first bit is sent out from the source.

- By Bandwidth and delay, we measure the performance of a network. In data communication, the product of bandwidth and delay is very important.
- Jitter is related to variations in delay.
- Line coding is the process of converting digital data to digital signals. Line coding converts the sequence of bits to a digital signal.
- We can divide line coding schemes into three basic categories: uni-polar, polar and bi-polar.
- In unipolar, all the signal levels are on one side of the time axis, either above or below.
- In polar schemes, the voltages are on both sides of the time axis. It uses two voltage levels – one positive and the other one negative. Four different encoding schemes: NRZ, RZ, Manchester and Differential Manchester.
- The transmission of binary data across a link can be done in either parallel or serial mode.
- In serial mode, one bit is sent with each clock tick.
- In parallel transmission, there is only one method to send data.
- In serial transmission, there are three methods of sending data: asynchronous, synchronous and isochronous.
- In asynchronous transmission, we send 1 start bit (0) at the beginning and 1 or more stop bits (1s) at the end of each byte.
- In synchronous transmission, we send bits one after another without start or stop bits or gaps. It is the responsibility of the receiver to group the bits.
- The isochronous mode provides synchronization for the entire stream of bits. In other words, it guarantees that the data arrive at a fixed rate.
- Multiplexing is a technique by which different analog and digital streams of transmission can be simultaneously processed over a shared link. There are three basic multiplexing techniques: Frequency division multiplexing, Wavelength division multiplexing and Time 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.
- Wavelength-division multiplexing (WDM) is designed to use the high bandwidth capability of fiber-optic cable. WDM is an analog multiplexing technique to combine optical signals.
- Time-division multiplexing (TDM) is a digital process that allows several connections to share the high bandwidth of a link. TDM is a digital multiplexing technique for combining several low-rate channels into one high-rate one.

- Switching is process to forward packets coming in from one port to a port leading towards the destination
- The switching performed by different nodes can be categorized into the following three types: Circuit Switching, Packet Switching and Message Switching.

Check Your Understanding

1. _____ encoding has a transition at the beginning of each 0 bit.
   (a) Differential Manchester (b) RZ
   (c) Manchester (d) All the above.
2. Which of the following is NOT a clause of impairment?
   (a) Attenuation (b) Bandwidth
   (c) Distortion (d) Noise.
3. Bipolar encoding involves _____ signal levels.
   (a) Five (b) Four
   (c) Three (d) Two.
4. Which type of noise is caused due to spikes ?
   (a) Thermal (b) Induced
   (c) Crosstalk (d) Impulse.
5. Which of the following encoding schemes does not take care of synchronization?
   (a) Manchester (b) RZ
   (c) NRZ-L (d) NRZ-I.
6. A telephone network is an example of a _____ network.
   (a) Circuit-switched (b) Packet-switched
   (c) Message-switched (d) None of the above.
7. Which of the switching mechanisms delivers packets in order?
   (a) Packet and Message (b) Circuit and Packet
   (c) Packet (d) Circuit.
8. The internet uses which types of subnet?
   (a) Circuit switched (b) Packet switched
   (c) Message switched (d) None of the above.

ANSWER KEY

1. (a)	2. (b)	3. (c)	4. (d)	5. (c)
6. (a)	7. (d)	8. (b)		

Practice Questions

Q.1: Answers the Following Questions in short.

1. What is baseband transmission?
2. List the causes of signal impairment.
3. List the services of the physical layer.
4. What are the two forms of signaling?
5. Write the formula for calculating attenuation.
6. List the types of noise that affect data signals.
7. Write the Nyquist and Shannon's formula for calculating data rate of a channel.
8. Calculate maximum bit rate using Shannon's Theorem for a channel having bandwidth 31000 Hz and S/N ratio 20 dB
9. List the important criterias for measuring network performance.
10. Write the formula for calculating latency.
11. What is synchronous and asynchronous transmission?

Q.2: Answers the Following Questions.

1. List the different delays that can occur during transmission.
2. What are the various encoding schemes?
3. What is the difference between Manchester and Differential Manchester encoding?
4. What is the difference between NRZ-L and NRZ-I codes?
5. List the transmission modes.
6. List three different techniques in serial transmission and explain the differences.
7. What is the difference between serial and parallel transmission?
8. What is the main difference between frequency and time division multiplexing?
9. What are the different types of switching?
10. What are the disadvantages of unipolar encoding?
11. Draw NRZ-L encoding for 01001010 bit pattern.
12. Draw NRZ-I bit pattern for 01011100.
13. Draw the NRZ - Land Manchester encoding for the following data stream: 01010101.
14. Show Manchester and differential Manchester encoding pattern for the bit stream 10111000.
15. What are different switching techniques?
16. Compare circuit switching and packet switching.

Q.3: Define the terms.

1. Digital signal
2. Analog signal
3. Unipolar encoding
4. Line coding
5. Bit rate
6. Bit length
7. Switching
8. Multiplexing
9. Jitter
10. Latency
11. Noise
12. Distortion
13. Attenuation
14. Baseband transmission
15. Broadband transmission

Previous Exams Questions

Summer 2019

1. Most packet switches use this principle: **[1M]**

(i) Stop and wait

(ii) Store and forward

(iii) Both stop and wait and store and forward

(iv) None of the above

2. What is Multiplexing ? **[1M]**

Ans. Refer to section 3.9

3. What is FDM ? **[1M]**

Ans. Refer to section 3.9.1

4. Define the following terms: **[3 M]**

(i) Jitter – Refer to section 3.6.5

(ii) Bit length - Refer to section 3.2.3

(iii) Bit interval - Refer to section 3.2.3

5. Explain message switching in detail. **[4 M]**

Ans. Refer to section 3.10.2

6. Explain line coding schemes - NRZ. **[4 M]**

Ans. Refer to section 3.7.2

7. Explain TDM in detail. **[3 M]**

Ans. Refer to section 3.9.2

8. Explain line coding characteristics. **[5 M]**

Ans. Refer to section 3.7.1

9. Give a channel with an intended capacity of 20 Mbps. The bandwidth of channel is 3 MHz. What signal to noise ratio is required in order to achieve this capacity? **[3 M]**

Ans. Refer to Example 8

10. Explain performance of Network Bandwidth. **[4 M]**

Ans. Refer to section 3.6.1

11. Explain different transmission modes in detail. **[3 M]**

Ans. Refer to section 3.8

Winter 2018

1. Which type of noise is caused due to spikes ? **[1M]**

(i) Thermal (ii) Crosstalk

(iii) Induced **(iv) Impulse**

2. What is digital signal ? **[1M]**

Ans. Refer to section 3.2.2

3. Draw graph for NRZ-L, NRZ-I coding for the following data: **[4 M]**

(1) 00000000 (2) 11111111

(3) 01010101 (4) 00110011.

Ans. Refer to Example 13

4. What is Noise ? Explain with diagram. **[4 M]**

Ans. Refer to section 3.4.3

5. List important criterias for measuring network performance. **[3 M]**

Ans. Refer to section 3.6

6. What are different switching techniques ? Explain any one of them in detail. **[4 M]**

Ans. Refer to section 3.10

7. A channel with an intended capacity of 20 mbps. The bandwidth of the channel is 3 MHz. What signal-to-noise ratio is required in order to achieve this capacity?

Ans. Refer to Example 8. **[4 M]**

Summer 2018

1. A telephone network is an example of a _____ network. **[1 M]**

(i) Circuit-switched (ii) Packet-switched

(iii) Message-switched (iv) None of the above.

2. Define bit rate and bit length. **[1 M]**

Ans. Refer to section 3.2.3

3. Define the following terms: **[3 M]**

(i) Bit rate – Refer to section 3.2.3

(ii) Bit length - Refer to section 3.2.3

(iii) Bit interval - Refer to section 3.2.3

4. Explain line coding characteristics. What is unipolar line coding scheme? Give its drawbacks. **[5 M]**

Ans. Refer to section 3.7

5. Explain the different modes of transmission. **[3 M]**

Ans. Refer to section 3.8

6. Draw graph for NRZ-I coding for following data. **[3 M]**

(i) 00000000 (ii) 01010101 (iii) 00110011

Ans. Refer to Example 13.

❖❖❖

4...

Data Link Layer

Objectives...

- To study Error Detecting Techniques.
- To study Elementary Data Link Protocols.
- To learn Sliding Window Protocol.
- To study Protocols used in Random Access Method.
- To understand Protocols used in Controlled Access Method.
- To learn Protocols used in Channelization Access Method.

4.1 INTRODUCTION

- The Data Link Layer is the second layer in the OSI model, above the Physical Layer, which ensures that the error free data is transferred between the adjacent nodes in the network.
- It breaks the datagram passed down by above layers and converts them into frames ready for transfer. This is called Framing.
- It provides following two main functionalities:
  1. Reliable data transfer service between two peer network layers.
  2. Flow Control mechanism which regulates the flow of frames such that data congestion is not there at slow receivers due to fast senders.
- So Data link layer has two sub-layers:
  1. Logical Link Control (LLC): It deals with protocols, flow-control, and error control.
  2. Media Access Control (MAC): It deals with actual control of media.

4.2 FRAMING

- Data link layer is intermediate between network layer and physical layer.
- To provide service to the network layer, the data link layer must use the service provided to it by the physical layer.
- Physical layer accepts raw bit stream which is not guaranteed to be error free, and attempt it to deliver it to the destination.

- So it is the responsibility of data link layer to detect errors such as number of bits received may be less or contain different values etc.
- The data link layer breaks the bit stream into the frames and compute checksum for each frame. When frame comes at destination, the checksum is recomputed, if it is different, an error has occurred and it will be corrected.

4.2.1 Framing Concept

- A frame is a digital data transmission unit in computer networking.
- The data link layer divides the continuous bit stream that physical layer uses into units called frames, and computes the checksum for each frame and puts it as a field called Frame Check Sequence (FCS) in the frame format, i.e. the way bits are organized in the frame.
- At the destination, the checksum is recomputed when the frame arrives. This facilitates error detection.
- Recognizing the frame boundaries as a synchronous bit pattern arrives is called framing.
- The data link layer accepts the bit stream from the physical layer and breaks it into frames, this process is known as framing.
- Fig. 4.1 shows frame format in data link layer.

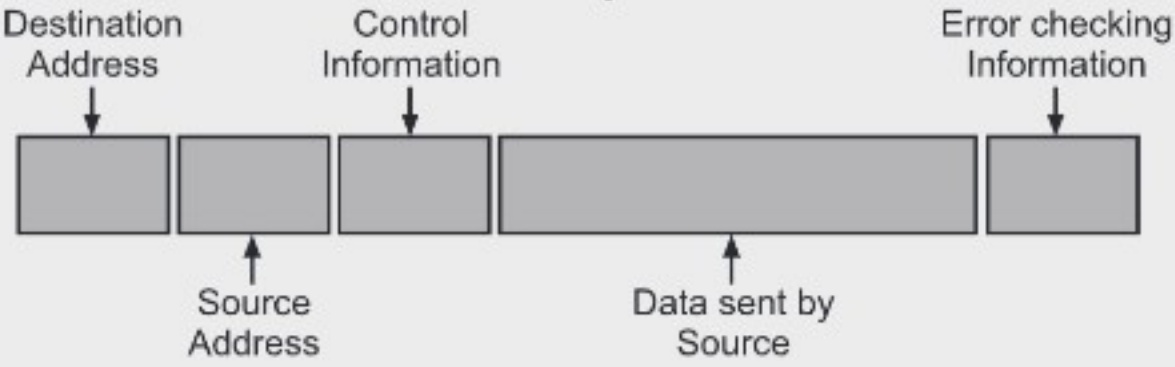


Fig. 4.1: Frame Format

4.2.2 Framing Methods (S-18, 19)

- We will study following three methods of framing:
  1. Character count.
  2. Flag bytes with byte stuffing.
  3. Starting and ending flags, with bit stuffing.

4.2.2.1 Character Count

- It uses a field in the header to specify the number of characters in the frame.
- When the data link layer at the destination see the character count, it knows how many character follows and where the end of frame is.
- The following Fig. 4.2 shows four frames of sizes 5, 5, 8 and 8 characters respectively.
- The problem with this method is the count can be garbled by a transmission error.

- In Fig. 4.2 (b), the character 5 in frame 2 becomes 7, so destination frames get out of synchronization and is unable to locate the start of the next frame.

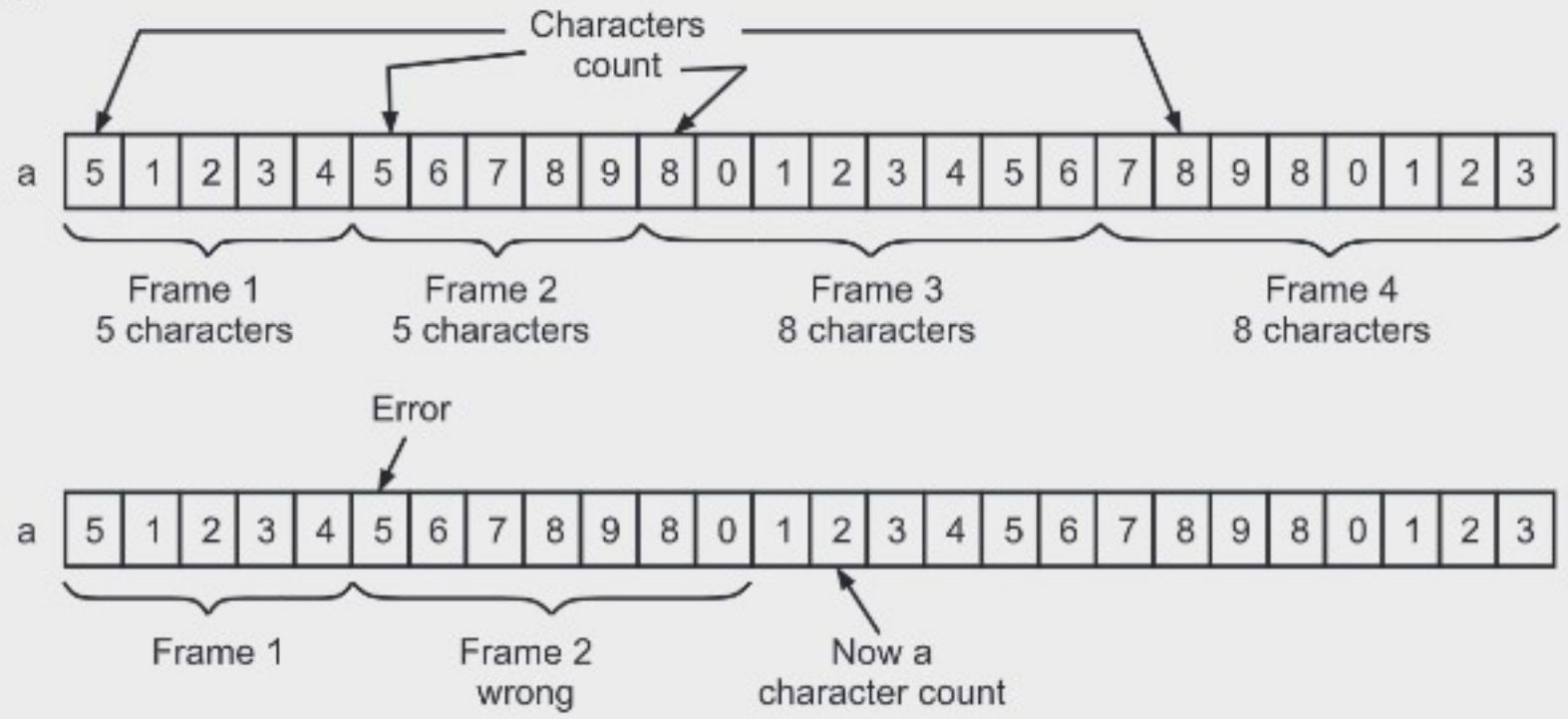


Fig. 4.2: A Character Stream (a) Without Error, (b) With One Error

- So in case of any error, the entire data has to be retransmitted. But retransmission does not help either, since the destination does not know how many characters to skip over to get to the start of the retransmission. For this reason, the character count method is rarely used anymore.

4.2.2.2 Flag Bytes with Byte Stuffing

- This method solves the problem of resynchronization.
- Each frame start and end with special bytes called flag byte.
- The flag byte is used as starting and ending delimiter as shown in Fig. 4.3.

(a) A Frame Delimited by Flag Bytes

(b) Four Examples of Byte Sequences

Fig. 4.3

- If the receiver loses synchronization, it can just search the FLAG byte to find the end of the current frame. Two consecutive flag bytes indicate the end of one frame and start of next frame.
- A problem here comes with the binary data or floating point numbers are being transmitted. It may easily happen that the flag byte's bit pattern occurs in the data. This situation will usually interfere with the framing. One way to solve this, a special ESC byte is inserted just before each accidental flag byte in the data. The data link layer on the receiving end remove the escape byte before the data are given to the network layer. This is known as **byte stuffing** or **character stuffing**.
- A major drawback is it uses 8-bit characters. Not all character codes use 8-bit characters. Unicode uses 16-bit characters. So, it cannot be used for arbitrary sized characters.

4.2.2.3 Starting and Ending Flags with Bit Stuffing

- In this method, it allows character codes with an arbitrary number of bits per character. Each frame begins and ends with a special bit pattern, 01111110.
- Whenever the sender's data link layer-encounters a five consecutive 1s in the data, it automatically stuffs a 0-bit into the outgoing bit stream. So this is bit stuffing.
- When receiver sees 5 consecutive 1-bit followed by a 0-bit, it automatically destuffs the 0-bit.
- If the user data contain the flag pattern, 01111110, this is transmitted as 011111010 but stored in the receiver's memory as 01111110.
- With bit stuffing, the boundary between two frames can be unambiguously recognized by the flag pattern. Thus, if the receiver loses track of where it is, all it has to do is scan the input for flag sequences, since they can only occur at frame boundaries and never within the data.
- The Fig. 4.4 shows the bit stuffing.

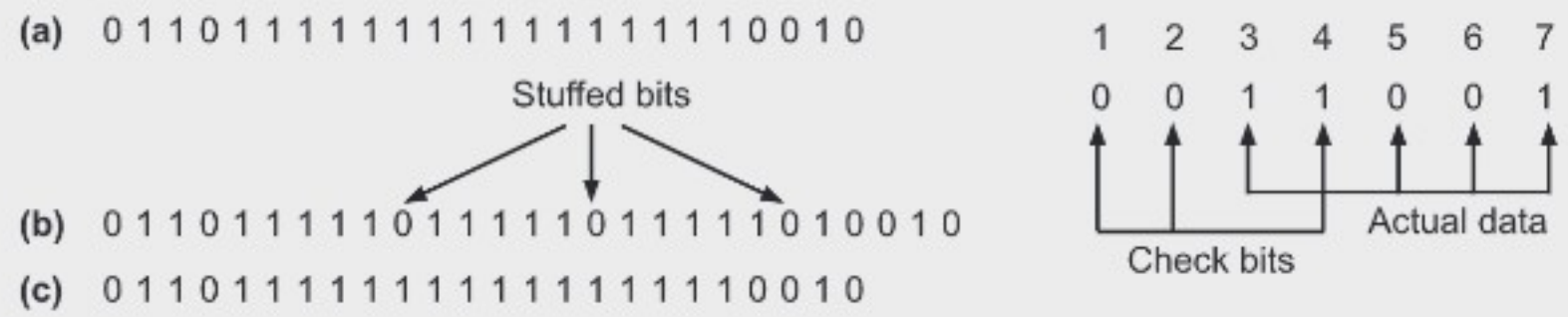


Fig. 4.4: (a) Original Data (b) The Data Appear on the Line (c) The Data at Receivers Site

4.3 ERROR DETECTION CODE

- As the signal is transmitted through a media, the signal gets corrupted because of noise and distortion. In other words, the media is not reliable. To achieve a reliable

communication through this unreliable media, there is need for detecting the error in the signal so that suitable mechanism can be devised to take corrective actions.

- The errors can be divided into two types: Single-bit error and Burst error. **(S-19)**

1. **Single-bit Error:** The term single-bit error means that only one bit of given data unit (such as a byte, character, or data unit) is changed from 1 to 0 or from 0 to 1.

- In a frame, there is only one bit, anywhere though, which is corrupt.

Fig. 4.5: Concept of Single-bit Error

2. **Burst Error:** The term burst error means that two or more bits in the data unit have changed from 0 to 1 or vice-versa. Note that burst error doesn't necessary means that error occurs in consecutive bits.

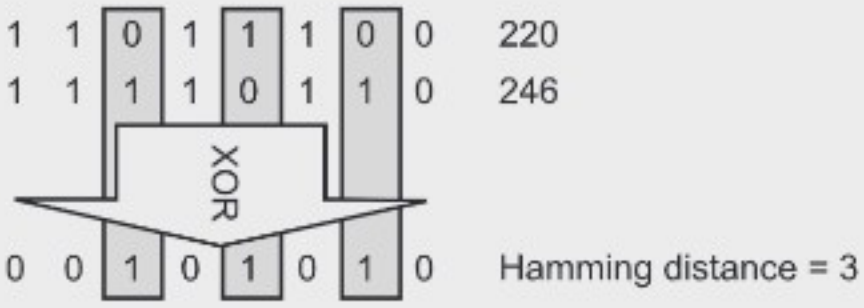
- Frame contains more than 1 consecutive bits corrupted.

Fig. 4.6: Concept of Burst Error

- There are two ways for dealing with errors:
  1. **Error Correcting Codes:** Include some redundant information along with each block of data so that receiver can know what the transmitted data must have been.
  2. **Error Detecting Codes:** Here, only enough redundant information is added with data so the receiver can know that error has occurred but not which error, and can request a retransmission.

4.3.1 Hamming Distance

- 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 it also corrects it.
- The Hamming distance between two words (of the same size) is the number of differences between the corresponding bits. The Hamming distance between two words x and y is shown as d(x, y). In other words, the Hamming distance between the received codeword and the sent codeword is the number of bits that are corrupted during transmission.
- The Hamming distance can easily be found if we apply the XOR operation on the two words and count the number of 1s in the result. Note that the Hamming distance is a value greater than zero.
- If two codewords are a Hamming distance d-apart, it will require d single-bit errors to convert one codeword to other. The error detecting and correcting properties depends on its Hamming distance.



- For example, if the codeword 00000 is sent and 01101 is received, the Hamming distance between the two is d(00000, 01101) = 3 because 00000 ⊕ 01101 is 01101 (three 1's)
- The Hamming distance d(10101, 11110) is 3 because 10101 ⊕ 11110 is 01011

Minimum Hamming Distance:

- The minimum Hamming distance is the smallest Hamming distance between all possible pairs. To find this value, we find the Hamming distances between all words and select the smallest one.
- To detect d errors, you need a distance (d+1) code because with such a code there is no way that d-single bit errors can change a valid codeword into another valid codeword. Whenever receiver sees an invalid codeword, it can tell that a transmission error has occurred.
- Similarly, to correct d errors, you need a distance 2d+1 code because that way the legal codewords are so far apart that even with d changes, the original codeword is still closer than any other codeword, so it can be uniquely determined.

4.3.2 CRC (S-18, 19)

- The most popular error detection technique is based on polynomial is called as CRC (Cyclic Redundancy Check).
- In general, in this method, The transmitter generates an n-bit check sequence number from a given k-bit frame such that the resulting (k+n) bit frame is divisible by some number. The receiver divides the incoming frame by the same number. If the result of the division does not leave a remainder, the receiver assumes that there was no error.
- CRC is used by all advanced data link protocols, for the following reasons:
  1. Powerful error detection capability.
  2. CRC can be efficiently implemented in hardware.
- In CRC , bit strings are represented as polynomials with the coefficients of 0 and 1 only. A k-bit frame is a coefficient list for a polynomial with k terms, ranging from x^{k-1} to x^0. Such a polynomial is said to be of degree k-1.
- For example, 110001 has 6-bits so it will be represented as six term polynomial with the coefficients 1, 1, 0, 0, 0 and 1.So polynomial is $x^5 + x^4 + x^0$.
- Polynomial arithmetic is done modulo 2 according to the algebra theory. It does not have carries for addition or borrows for subtraction. Both addition and subtraction are identical to exclusive OR.

- When this technique is used, sender and receiver must agree upon a generator polynomial, G(x). High and low order bits must be 1. The checksum is appended in such a way that polynomial represented by the checksummed frame is divisible by G(x).
- When the receiver gets this frame, it divides it by G(x). If there is a remainder then there is a transmission error.
- To compute the CRC for some frame with m bits corresponding to the polynomial M(x), the algorithm for computing the CRC is as follows:
  1. Let r be the degree of G(x). Append r zero bits to the low-order end of the frame so it now contains m + r bits and corresponds to the polynomial $x^r M(x)$.
  2. Divide the bit string corresponding to G(x) into the bit string corresponding to x^r M(x), using modulo 2 division.
  3. Subtract the remainder (which is always r or fewer bits) from the bit string corresponding to x^r M(x) using modulo 2 subtraction. The result is the checksummed frame to be transmitted. Call its polynomial T(x).
- The Fig. 4.7 shows basic scheme of CRC.

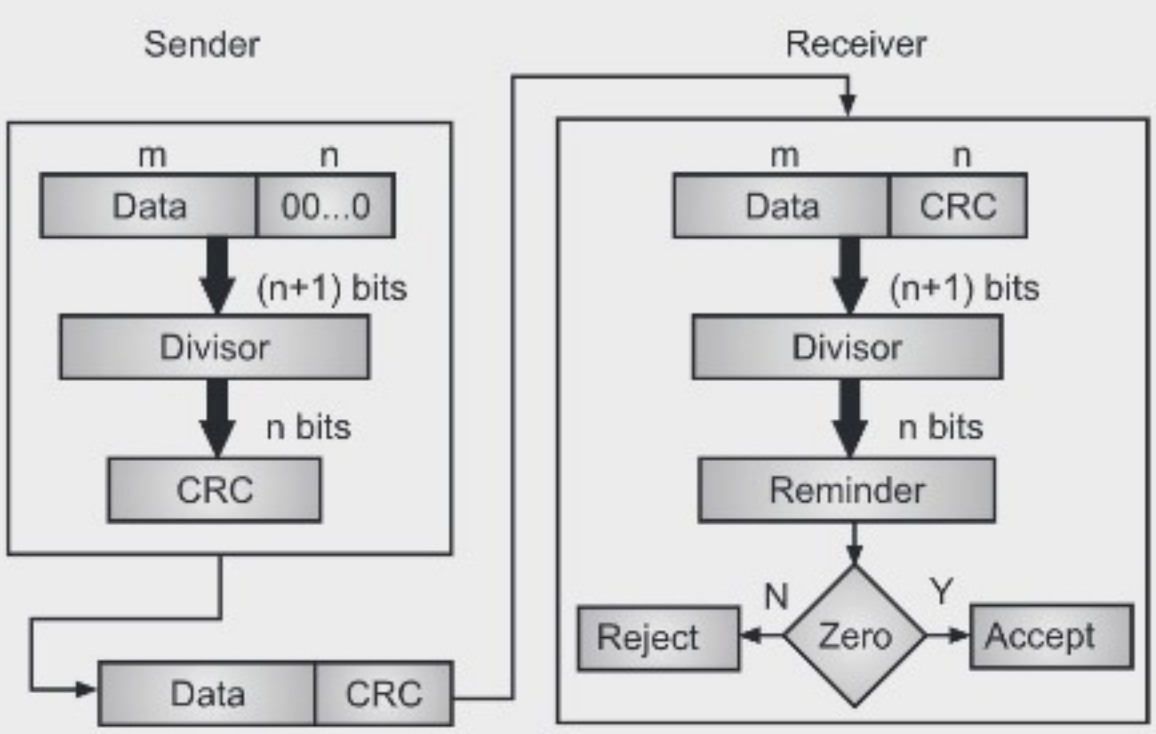


Fig. 4.7: Basic Scheme of CRC

- To understand this, we will study the following example. Suppose the message is 1101011011 and

$$G(x) = x^4 + x + 1$$

$$\therefore \quad \text{Generator} = 10011$$

The message after 4-bits appended is r = 4.

11010110110000

Now this stream is divided by the generator.

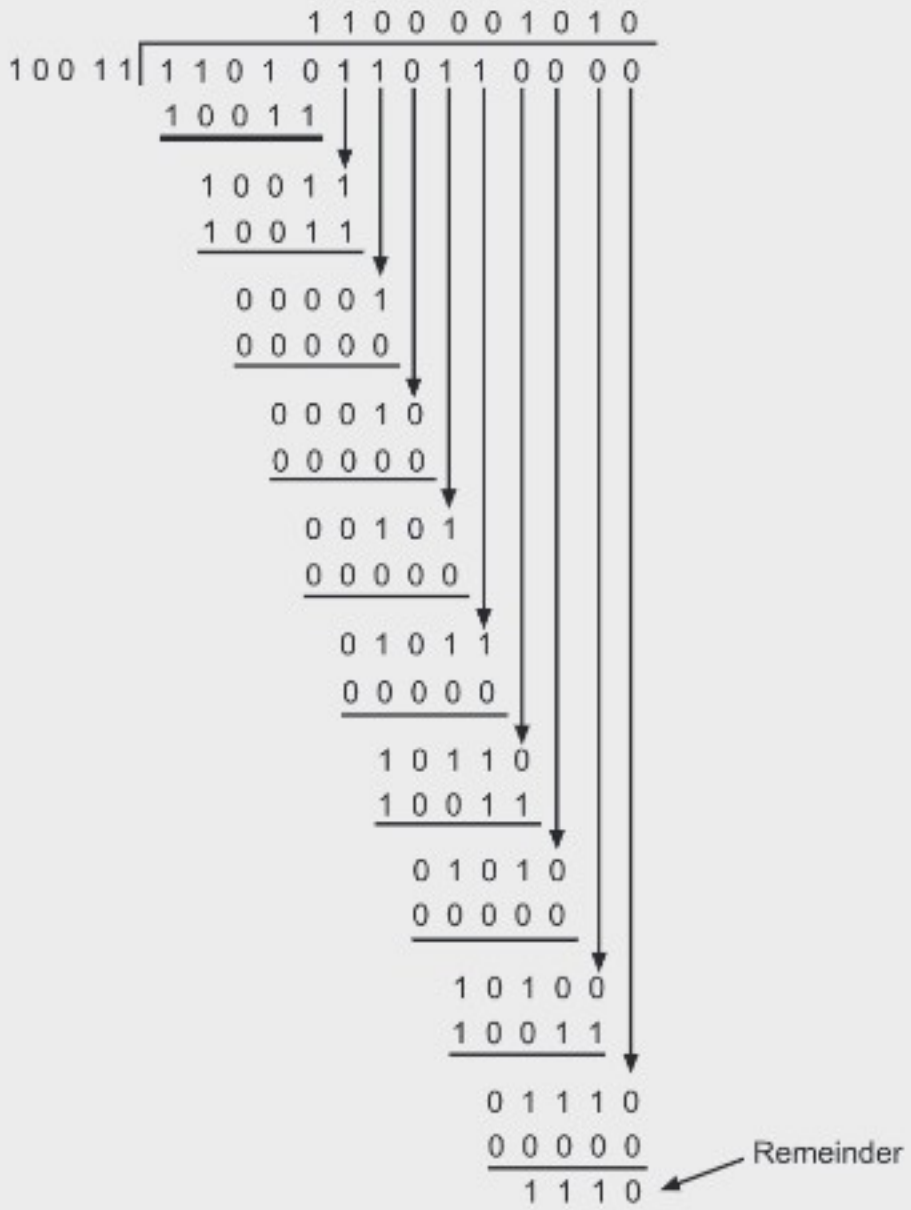


Fig. 4.8: Calculation of CRC

$$x^r M(x) = 11010110110000$$
$$\text{Remainder} = \quad - 1110$$
$$T(x) = 11010110111110$$

Thus the transmitted frame is 11010110111110.

- Actual data bits plus the remainder is called a codeword. The sender transmits data bits as codewords. At the other end, the receiver performs division operation on codewords using the same CRC divisor. If the remainder contains all zeros the data bits are accepted, otherwise it is considered as there is some data corruption occurred in transit.

Points to note in CRC:

1. The only relationship between the size of the codeword and dataword is the one based on the definition: n = k + r, where n is the size of the codeword, k is the size of the dataword, and r is the size of the remainder.
2. The remainder is always one bit smaller than the divisor.
3. The degree of the generator polynomial is one less than the size of the divisor. For example, the CRC-32 generator (with the polynomial of degree 32) uses a 33-bit divisor.
4. The degree of the generator polynomial is the same as the size of the remainder (length of checkbits). For example, CRC-32 (with the polynomial of degree 32) creates a remainder of 32 bits.

- A polynomial is selected to have at least the following properties:
  - It should not be divisible by X.
  - It should not be divisible by (X+1).
- The first condition guarantees that all burst errors of a length equal to the degree of polynomial are detected. The second condition guarantees that all burst errors affecting an odd number of bits are detected.
- Commonly used divisor polynomials are:

CRC-12: $P(X) = X^{12} + X^{11} + X^3 + X^2 + X + 1$

CRC-16: $P(X) = X^{16} + X^{15} + X^2 + 1$

CRC-CCITT: $P(X) = X^{16} + X^{12} + X^5 + 1$

CRC-32: $P(X) = X^{32} + X^{26} + X^{23} + X^{22} + X^{16} + X^{12} + X^{11} + X^{10} + X^8 + X^7 + X^5 + X^4 + X^2 + X + 1$

Performance:

- CRC is a very effective error detection technique. If the divisor is chosen according to the previously mentioned rules, its performance can be summarized as follows:
  - CRC can detect all single-bit errors.
  - CRC can detect all double-bit errors (three 1's).
  - CRC can detect any odd number of errors (X+1).
  - CRC can detect all burst errors of less than the degree of the polynomial.
  - CRC detects most of the larger burst errors with a high probability.

Example 1: Given the dataword 1010011110 and the divisor 10111. **(S-18)**

(a) Show the generation of the codeword at the sender site (using binary division).

(b) Show the checking of the codeword at the receiver site (assume no error).

Solution: Fig. 4.9 shows solution for above problems (a) and (b).

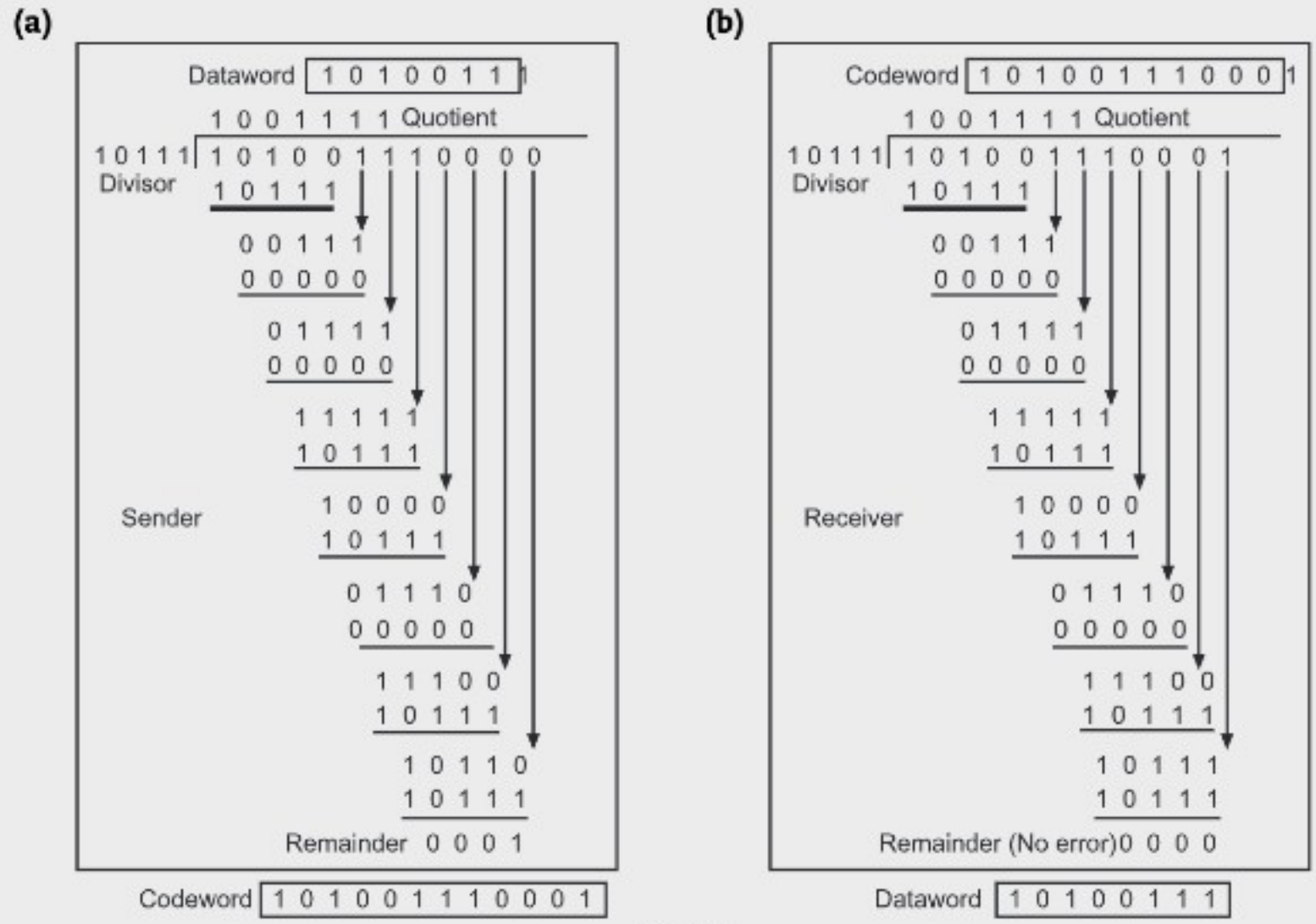


Fig. 4.9

Example 2: Dataword to be sent is 100100 and the divisor is 1101:

(a) Show the generation of the codeword at the sender side.

(b) Show the checking of the codeword at the receiver side.

Solution:

Sender Side:

```
          1 1 1 1 0 1
      ┌──────────────
1101  │ 1 0 0 1 0 0 0 0
        1 1 0 1
        ---------
          1 0 0 0
          1 1 0 1
          ---------
            1 0 1 0
            1 1 0 1
            ---------
              1 1 1 0
              1 1 0 1
              ---------
                0 1 1 0
                0 0 0 0
                -------
                  1 1 0 0
                  1 1 0 1
                  -------
                    0 0 1
```

Therefore, the remainder is 001 and hence the codeword sent is 100100001.

Receiver Side: Let there be error in transmission media. Codeword received at the receiver side is 100000001.

```
          1 1 1 0 1 0
      ┌──────────────
1101  │ 1 0 0 0 0 0 0 1
        1 1 0 1
        ---------
          1 0 1 0
          1 1 0 1
          ---------
            1 1 1 0
            1 1 0 1
            ---------
              0 1 1 0
              0 0 0 0
              -------
                1 1 0 0
                1 1 0 1
                -------
                  0 0 1 1
                  0 0 0 0
                  -------
                    0 1 1
```

- Since the remainder is not all zeroes, the error is detected at the receiver side.

4.4 ELEMENTARY DATA LINK PROTOCOLS

- Data Link Control is the service provided by the Data Link Layer to provide reliable data transfer over the physical medium. For example, In the half-duplex transmission mode, one device can only transmit the data at a time.

- If both the devices at the end of the links transmit the data simultaneously, they will collide and leads to the loss of the information. The Data link layer provides the coordination among the devices so that no collision occurs.
- For reliable and efficient data communication a great deal of coordination is necessary between at least two machines. Some of the following constraints should be considered:
  - Both sender and receiver have limited speed.
  - Both sender and receiver have limited memory.

  It is necessary to satisfy the following requirements:
  - A fast sender should not overwhelm a slow receiver, which must perform a certain amount of processing before passing the data on to the higher level software.
  - If error occur during transmission, it is necessary to devise mechanism to correct it.
- The most important functions of Data Link layer to satisfy the above requirements are error control and flow control. Collectively, these functions are known as data link control.
- Flow Control is a technique so that transmitter and receiver with different speed characteristics can communicate with each other. Flow Control is a set of procedures that tells the sender how much data it can transmit before it must wait for an acknowledgment from the receiver. The flow of data should not be allowed to overwhelm the receiver. Receiver should also be able to inform the transmitter before its limits (this limit may be amount of memory used to store the incoming data or the processing power at the receiver end) are reached and the sender must send fewer frames.
- Hence, Flow control refers to the set of procedures used to restrict the amount of data the transmitter can send before waiting for acknowledgment. It ensures that a transmitting station, such as a server with higher processing capability, does not overwhelm a receiving station, such as a desktop system, with lesser processing capability. This is where there is an orderly flow of transmitted data between the source and the destination.
- Error Control involves both error detection and error correction. It is necessary because errors are inevitable in data communication, in spite of the use of better equipment and reliable transmission media based on the current technology. In the preceding section, we have already discussed how errors can be detected. When an error is detected, the receiver can have the specified frame retransmitted by the sender. This process is commonly known as Automatic Repeat Request (ARQ).
- Data link layer protocols combine framing, flow control, and error control to achieve the delivery of data from one node to another. By using any common programming

language protocols are implemented. These protocols are divided into two types i.e., for noiseless channel, and for noisy channel as shown in Fig. 4.10.

- There are two methods developed for flow control namely Stop-and-wait and Sliding-window.

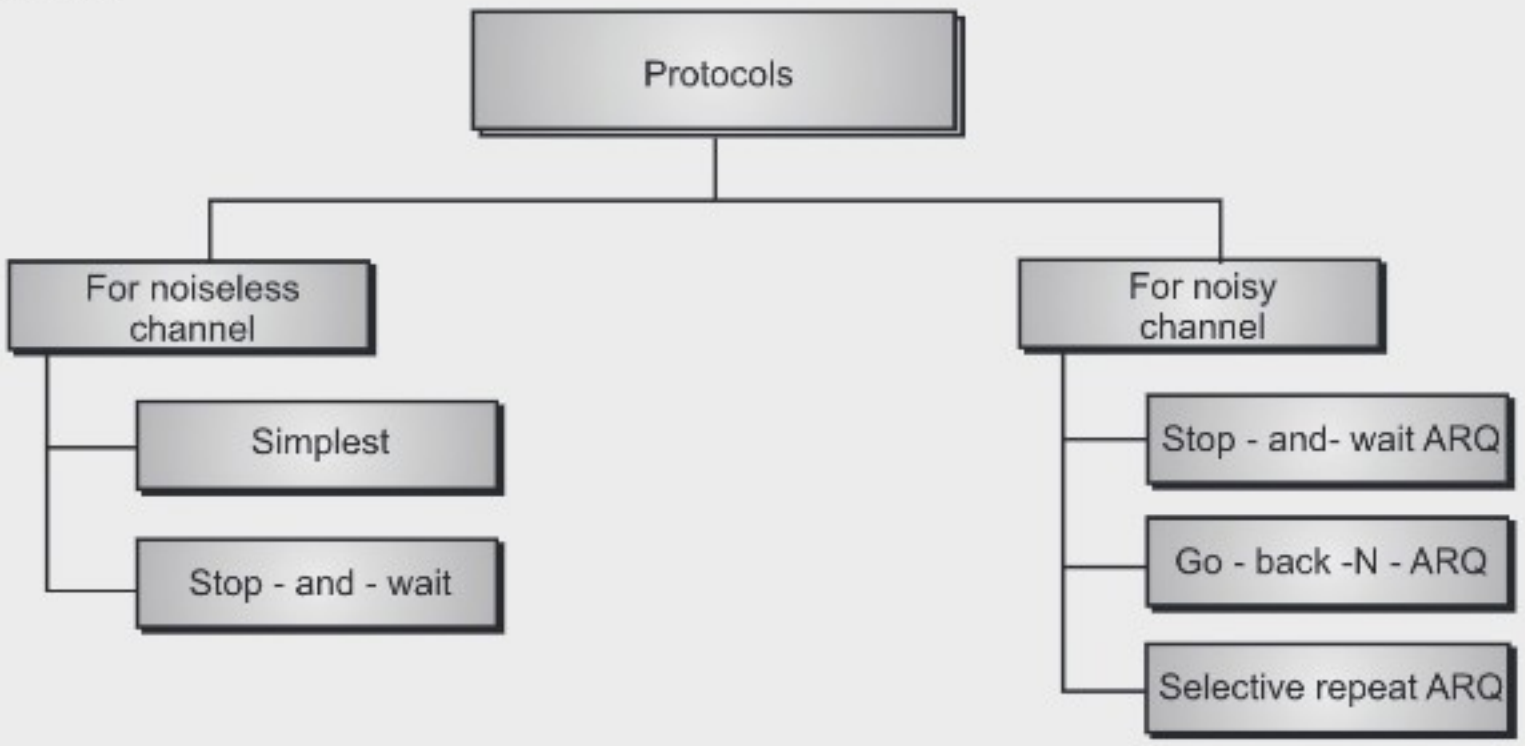


Fig. 4.10 Types of Protocol

- Stop-and-wait is also known as Request/reply sometimes. Request/reply (Stop-and-wait) flow control requires each data packet to be acknowledged by the remote host before the next packet is sent.
- Sliding window algorithms, used by TCP, permit multiple data packets to be in simultaneous transit, making more efficient use of network bandwidth.

4.4.1 Simplex Protocol

- This protocol is a simple but unrealistic protocol. It assumes that an ideal channel exists in which no frames are lost, duplicated, or corrupted.
- In this protocol:
  - It has no flow or error control.
  - It is a unidirectional protocol in which data frames are traveling in only one direction-from the sender to receiver.
  - The sender and receiver are always ready.
  - Processing time can be ignored.
  - Infinite buffer space is available.
  - No errors occur; i.e. no damaged frames and no lost frames (perfect channel).
  - The data link layer of the receiver immediately removes the header from the frame and hands the data packet to its network layer, which can also accept the packet immediately.

Design:

- The sender site cannot send a frame until its network layer has a data packet to send. The receiver site cannot deliver a data packet to its network layer until a frame arrives.
- The data link layer at the sender site gets data from its network layer, makes a frame out of the data, and sends it.
- The data link layer at the receiver site receives a frame from its physical layer, extracts data from the frame, and delivers the data to its network layer.

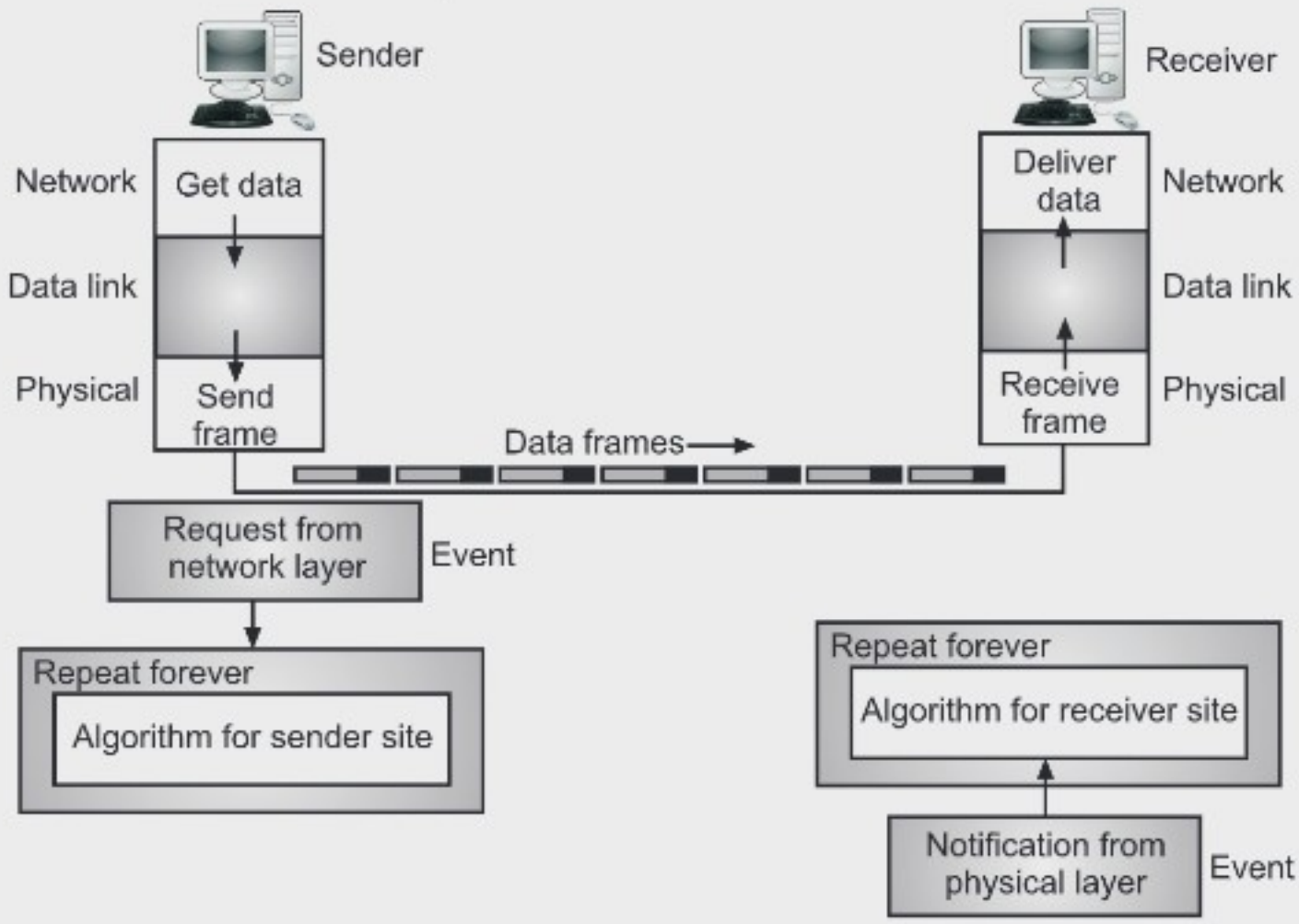


Fig. 4.11: The design of the simplest protocol with no flow or error control

- If the protocol is implemented as a procedure, There is need to introduce the idea of events in the protocol. The procedure at the sender site is constantly running; there is no action until there is a request from the network layer. The procedure at the receiver site is also constantly running, but there is no action until notification from the physical layer arrives.

4.4.2 Stop-and-Wait Protocol

- Flow control deals with problem that sender transmits frames faster than receiver can accept, and solution is to limit sender into sending no faster than receiver can handle.
- In this protocol, assumptions are as follows:
  - Data are transmitted in one direction only.
  - No errors occur (perfect channel).

- The receiver can only process the received information at a finite rate.
- These assumptions imply that the transmitter cannot send frames at a rate faster than the receiver can process them.

Working:

- This is the simplest form of flow control where a sender transmits a data frame.
- After receiving the frame, the receiver indicates its willingness to accept another frame by sending back an ACK frame acknowledging the frame just received.
- The sender must wait until it receives the ACK frame before sending the next data frame. This is sometimes referred to as ping-pong behavior, request/reply is simple to understand and easy to implement, but not very efficient.
- In LAN environment with fast links, this isn't much of a concern, but WAN links will spend most of their time idle, especially if several hops are required.

Design:

- The following Fig 4.12 shows the design of stop-and-wait protocol.

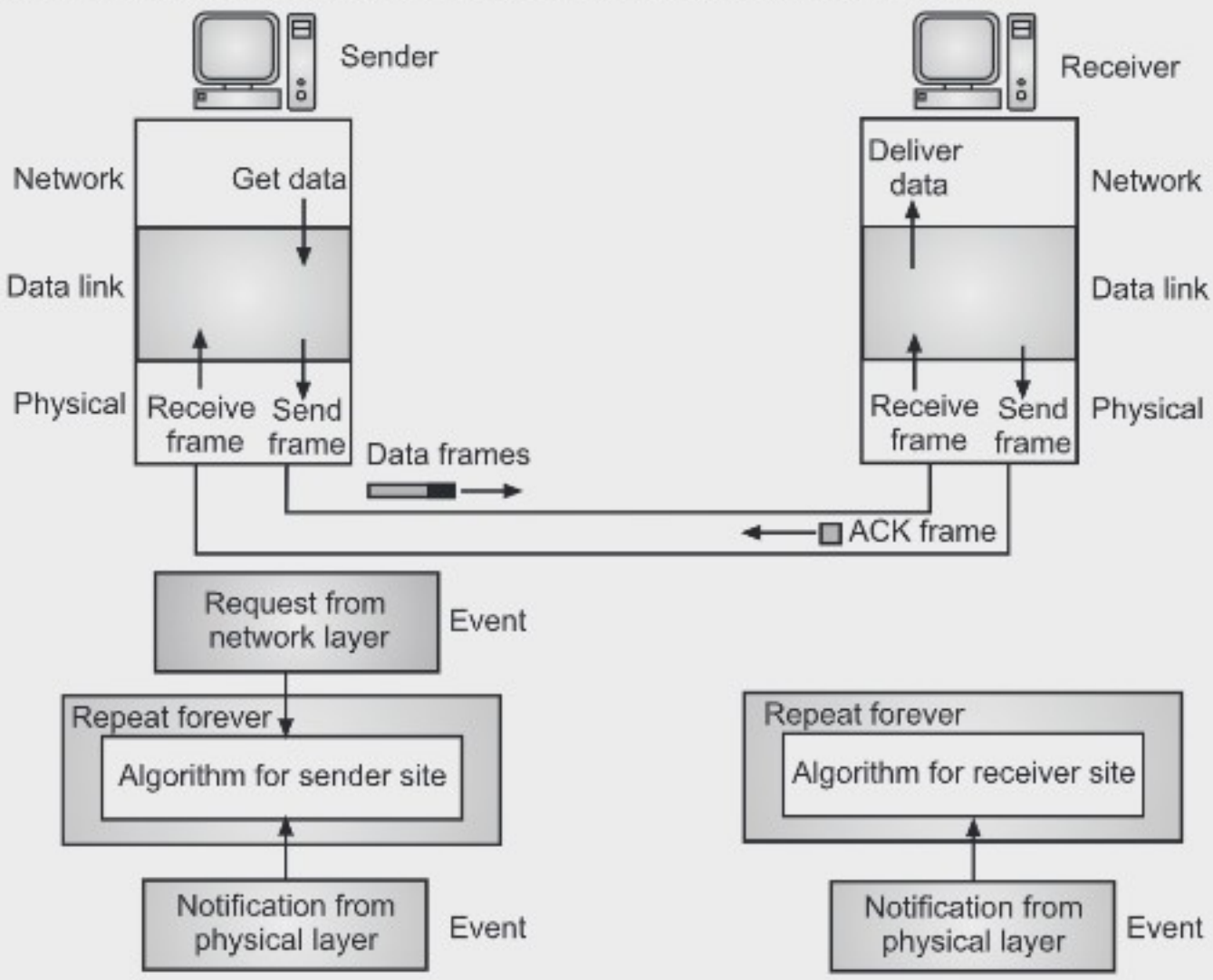


Fig. 4.12 Design of Stop-and-Wait Protocol

- In above figure, we can see the traffic on the forward channel (from sender to receiver) and the reverse channel. At any time, there is either one data frame on the forward channel or one ACK frame on the reverse channel. Therefore a half-duplex link is needed.

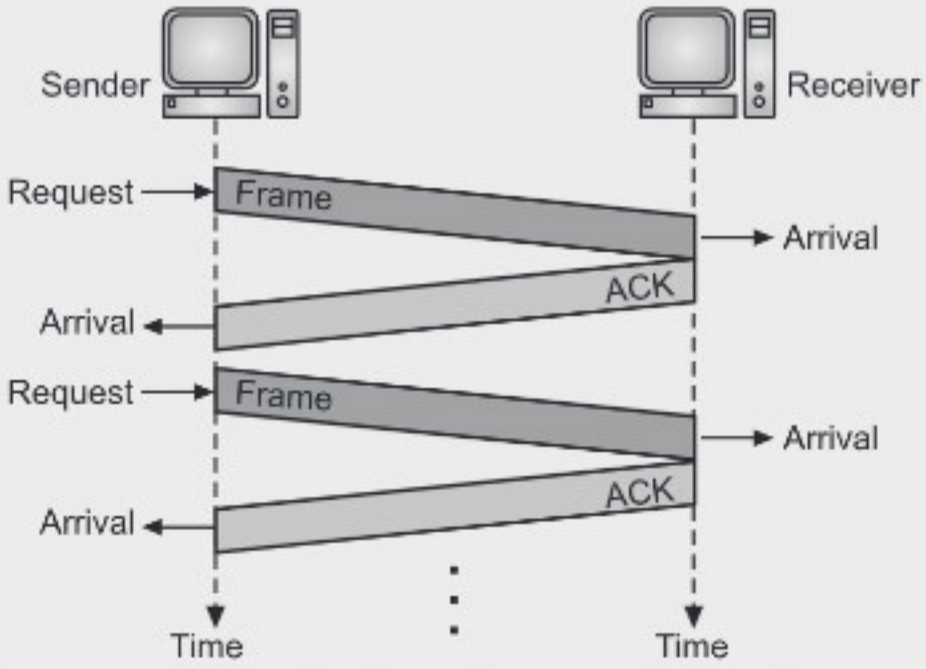


Fig. 4.13: Communication using Stop-and-Wait Protocol

- Above Fig. 4.13 shows an example of communication using Stop-and-Wait protocol. It is still very simple. The sender sends one frame and waits for feedback from the receiver. When the ACK arrives, the sender sends the next frame. Note that sending two frames in the protocol involves the sender in four events and the receiver in two events.

Advantages of Stop-and-Wait Protocol:

1. It is very simple to implement.
2. The main advantage of this protocol is the accuracy. The next frame is sent only when the first frame is acknowledged. So, there is no chance of any frame being lost.

Disadvantages of Stop-and-Wait Protocol

1. We can send only one packet at a time.
2. If the distance between the sender and the receiver is large then the propagation delay would be more than the transmission delay. Hence, efficiency would become very low.
3. After every transmission, the sender has to wait for the acknowledgment and this time will increase the total transmission time. This makes the transmission process slow.

4.4.3 Simplex Protocol for Noisy Channel

- When an error is detected in a message, the receiver sends a request to the transmitter to retransmit the ill-fated message or packet. The most popular retransmission scheme is known as Automatic Repeat Request (ARQ).
- Such schemes, where receiver asks sender to retransmit if it detects an error, are known as reverse error correction techniques. There exist three popular ARQ techniques.

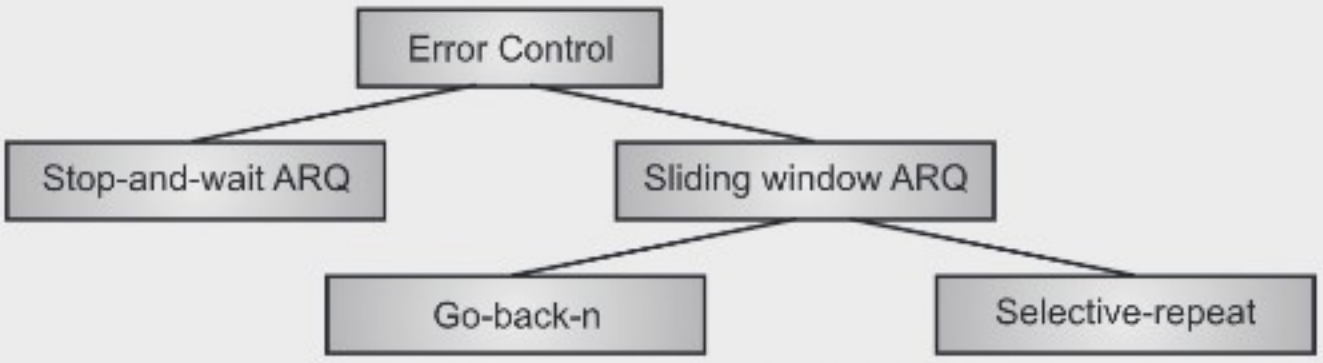


Fig. 4.14: Error control techniques

Stop-and-Wait Automatic Repeat Request

- The Stop-and-Wait Automatic Repeat Request (Stop-and-Wait ARQ), adds a simple error control mechanism to the Stop-and-Wait Protocol.

Working:

- A stop-and-wait ARQ sender sends one frame at a time.
- After sending each frame, the sender doesn't send any further frames until it receives an acknowledgement (ACK) signal.
- After receiving a good frame, the receiver sends an ACK.
- If the ACK does not reach the sender before a certain time, known as the timeout, the sender sends the same frame again.
- To detect and correct corrupted frames, there is need to add redundancy bits to data frame. Typically the transmitter adds a redundancy check number to the end of each frame.
- The receiver uses the redundancy check number to check for possible damage. If the receiver sees that the frame is good, it sends an ACK.
- If the receiver sees that the frame is damaged, the receiver discards it and does not send an ACK—pretending that the frame was completely lost, not merely damaged
- Stop and wait ARQ includes the following extra elements:

Time out timer

- The corrupted and lost frames need to be resent in this protocol. If the receiver does not respond when there is an error, how can the sender know which frame to resend? To solve this problem, the sender keeps a copy of the sent frame. At the same time, it starts a timer. If the timer expires and there is no ACK for the sent frame, the frame is resent, the copy is held, and the timer is restarted. Since the protocol uses the stop-and-wait mechanism, there is only one specific frame that needs an ACK even though several copies of the same frame can be in the network.

Sequence Numbers

- The protocol specifies that frames need to be numbered. This is done by using sequence numbers. A field is added to the data frame to hold the sequence number of that frame. For example, if we decide that the field is m bits long, the sequence numbers start from 0, go to 2^m - 1, and then are repeated.

Acknowledgment Numbers

- Since the sequence numbers must be suitable for both data frames and ACK frames, the convention used is the acknowledgment numbers always announce the sequence number of the next frame expected by the receiver. For example, if frame 0 has arrived safe and sound, the receiver sends an ACK frame with acknowledgment 1 (meaning frame 1 is expected next). If frame 1 has arrived safe and sound, the receiver sends an ACK frame with acknowledgment 0 (meaning frame 0 is expected).

Design

- The Fig. 4.15 shows the design of the Stop-and-Wait ARQ Protocol.
- The sending device keeps a copy of the last frame transmitted until it receives an acknowledgment for that frame. A data frames uses a seq No (sequence number); an ACK frame uses an ack No (acknowledgment number). The sender has a control variable, which we call S_n (sender, next frame to send), that holds the sequence number for the next frame to be sent (0 or 1).

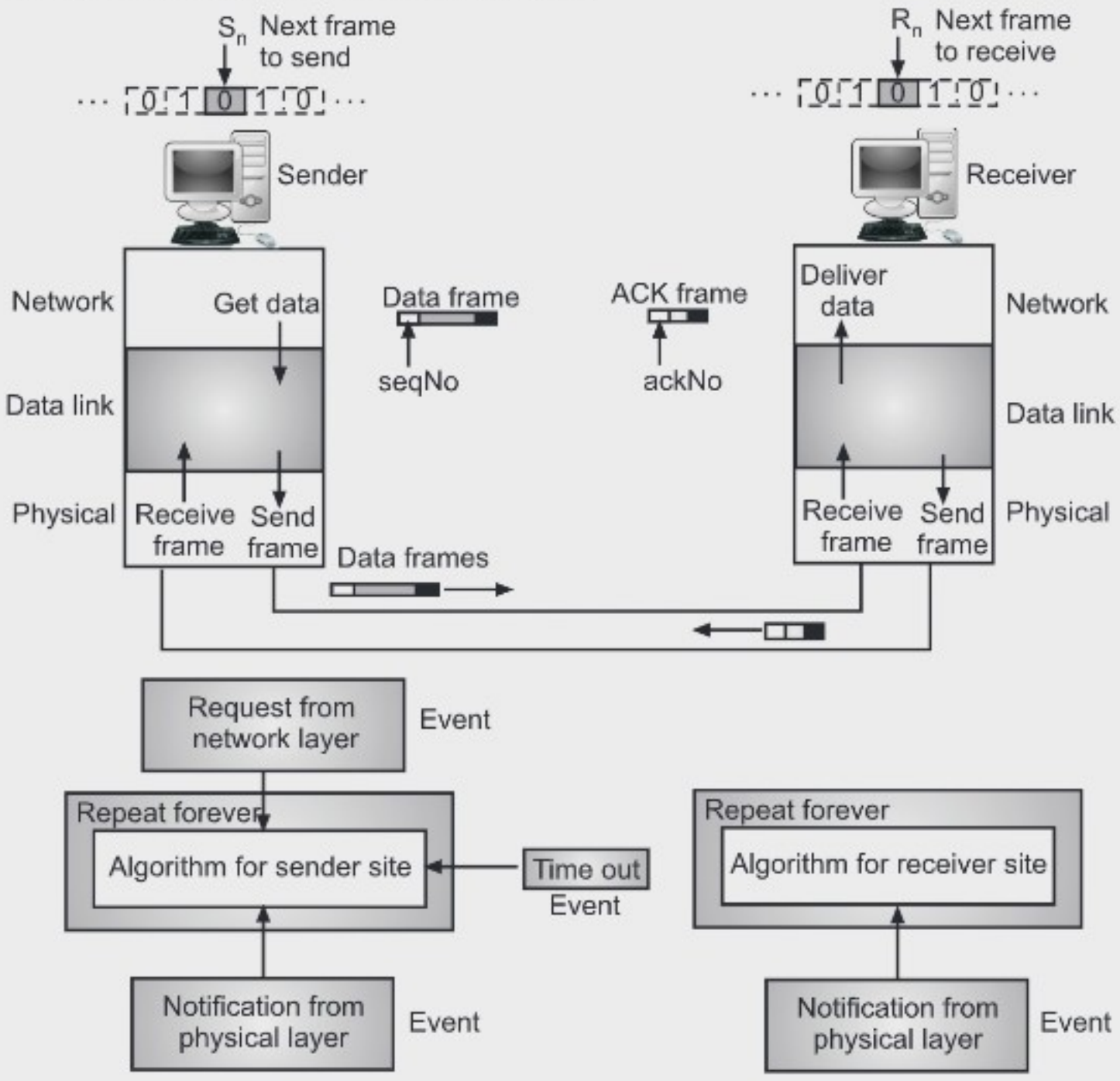


Fig. 4.15: Design of the Stop-and-Wait ARQ Protocol

- The receiver has a control variable, which we call R_n (receiver, next frame expected), that holds the number of the next frame expected. When a frame is sent, the value of S_n is incremented (modulo-2), which means if it is 0, it becomes 1 and vice versa. When a frame is received, the value of R_n is incremented (modulo-2), which means if it is 0, it becomes 1 and vice versa.
- In following figure, three events can happen at the sender site; one event can happen at the receiver site. Variable S_n points to the slot that matches the sequence number of the frame that has been sent, but not acknowledged; R_n points to the slot that matches the sequence number of the expected frame.
- **Example**: Frame 0 is sent and acknowledged. Frame 1 is lost and resent after the time-out. The resent frame 1 is acknowledged and the timer stops. Frame 0 is sent and acknowledged, but the acknowledgment is lost. The sender has no idea if the frame or the acknowledgment is lost, so after the time-out, it resends frame 0, which is acknowledged.

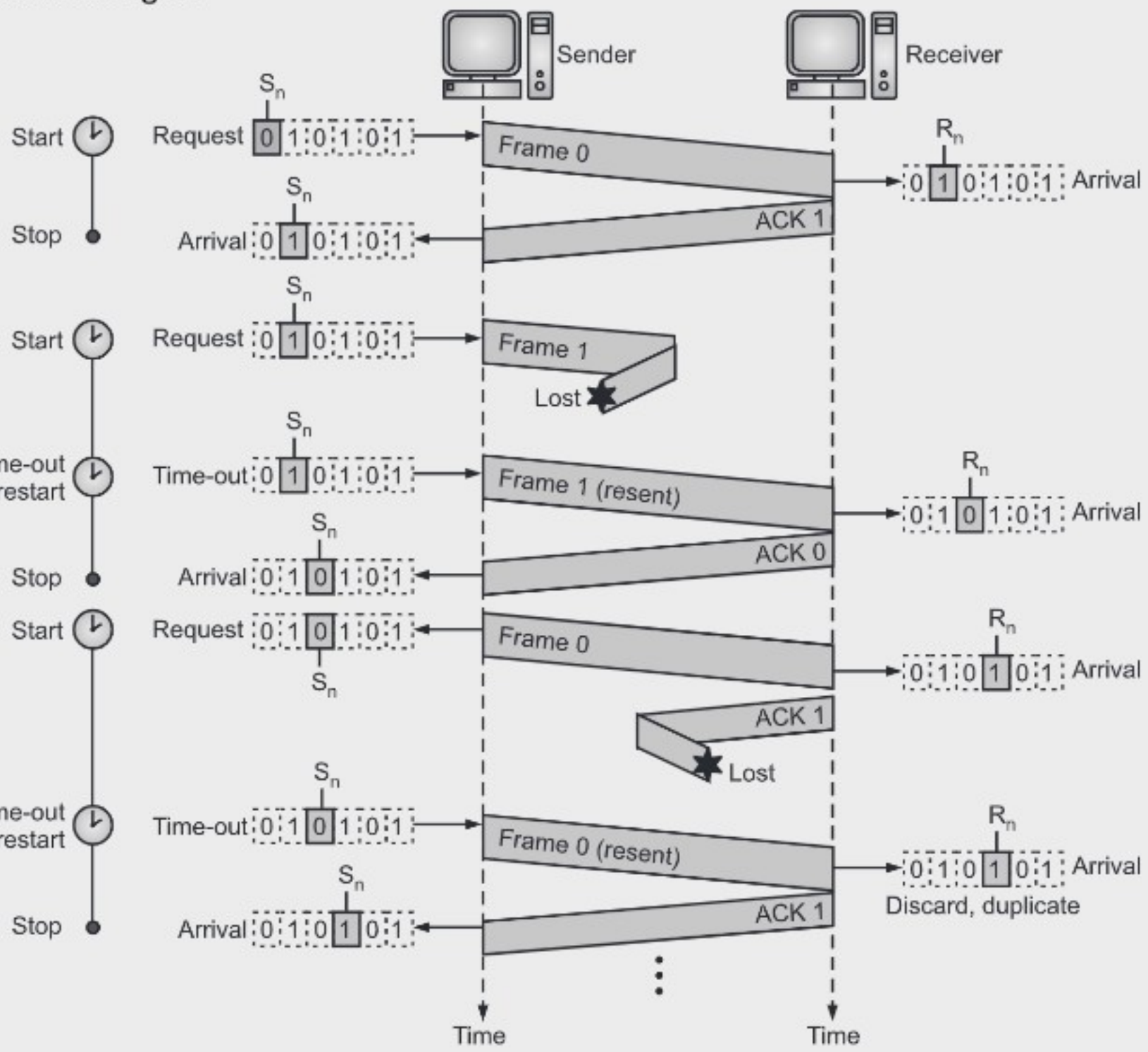


Fig. 4.16: Flow Diagram for above Example

Advantages of stop and wait protocol with ARQ:

1. It can be used for noisy channels.
2. It has both flow and error control mechanism.
3. It has timer implementation

Disadvantages of stop and wait protocol with ARQ:

1. Efficiency is very less.
2. Only one frame is sent at a time.
3. Timer should be set for each individual frame.
4. Sender and receiver window size is one.

Table 4.1: Difference between Stop and wait protocol & stop and wait ARQ

Sr. No.	Stop and Wait protocol	Stop and Wait ARQ
1.	It assumes that the communication channel is perfect and noise free.	It assumes that the communication channel is imperfect and noisy.
2.	Data packet sent by the sender can never get corrupt.	Data packet sent by the sender may get corrupt.
3.	There is no concept of negative acknowledgements.	A negative acknowledgement is sent by the receiver if the data packet is found to be corrupt.
4.	There is no concept of time out timer.	Sender starts the time out timer after sending the data packet.
5.	There is no concept of sequence numbers.	Data packets and acknowledgements are numbered using sequence numbers.

4.4.4 PPP (Point to Point Protocol)

- Point - to - Point Protocol (PPP) is a communication protocol of the data link layer that is used to transmit multiprotocol data between two directly connected (point-to-point) computers.
- It is a byte - oriented protocol that is widely used in broadband communications having heavy loads and high speeds.
- Since it is a data link layer protocol, data is transmitted in frames. It is also known as RFC 1661.
- PPP handles error detection, supports multiple protocols, allows IP addresses to be negotiated at connection time, permits authentication, and has many other features.

PPP provides several services:

1. PPP defines the format of the frame to be exchanged between devices and also defines how two devices can negotiate the establishment of the link and the exchange of data.
2. It also explain how network layer data are encapsulated in the data link frame.

3. It also authenticates two devices with each other.
4. PPP provides multiple network layer services supporting a variety of network layer protocols.
5. PPP provides connections over multiple links as well as network address configuration. This is particularly useful when a home user needs a temporary network address to connect to the Internet

PPP provides the following features:

1. A framing method that unambiguously delineates the end of one frame and the start of the next one. The frame format also handles error detection.
2. A link control protocol for bringing lines up, testing them, negotiating options, and bringing them down again gracefully when they are no longer needed. This protocol is called LCP (Link Control Protocol). It supports synchronous and asynchronous circuits and byte oriented and bit oriented encodings.
3. A way to negotiate network layer options in a way that is independent of the network layer protocol to be used. The method chosen is to have a different NCP (Network Control Protocol) for each network layer supported. The IP Control Protocol (IPCP) negotiates IP address assignments and other parameters when IP is used as network layer.
4. Authentication: It supports authentication. PPP supports two authentication protocols: Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP).

PPP Frame:

- PPP is a byte oriented protocol where each field of the frame is composed of one or more bytes. The following Fig.4.17 Shows PPP frame format. The fields of a PPP frame are –
  - **Flag:** 1 byte that marks the beginning and the end of the frame. The bit pattern of the flag is 01111110.
  - **Address**: 1 byte which is set to 11111111 in case of broadcast.
  - **Control**: 1 byte set to a constant value of 11000000.
  - **Protocol**: 1 or 2 bytes that define the type of data contained in the payload field.
  - **Payload**: This carries the data from the network layer. The maximum length of the payload field is 1500 bytes. However, this may be negotiated between the endpoints of communication.
  - **FCS**: It is a 2 byte or 4 bytes frame check sequence for error detection. The standard code used is CRC (Cyclic Redundancy Code)

Flag	Address	Control	Protocol	Payload	FCS	Flag
1 byte	1 byte (11111111)	1 byte (11000000)	1 or 2 byte	Variable	2 or 4 byte	1 byte (01111110)

Fig. 4.17: PPP Frame

- **Byte Stuffing in PPP Frame**: Byte stuffing is used PPP payload field whenever the flag sequence appears in the message, so that the receiver does not consider it as the end of the frame. The escape byte, 01111101, is stuffed before every byte that contains the same byte as the flag byte or the escape byte. The receiver on receiving the message removes the escape byte before passing it onto the network layer.

4.4.5 HDLC (High-Level Data Link Control)

- HDLC is a bit oriented protocol. It falls under the ISO standards ISO 3309 and ISO 4335. It specifies a packitization standard for serial links. It has been so widely implemented because it supports both half-duplex and full-duplex communication lines, point-to-point (peer to peer) and multi-point networks, and switched or non-switched channels. HDLC supports several modes of operation, including a simple sliding-window mode for reliable delivery. Other benefits of HDLC are that the control information is always in the same position, and specific bit patterns used for control differ dramatically from those in representing data, which reduces the chance of errors.
- HDLC operational Mode is the relationship between two devices involved in an exchange; the mode describes who controls the link. Exchanges over unbalanced configurations are always conducted in normal response mode. Exchanges over symmetric or balanced configurations can be set to specific mode using a frame design to deliver the command.
- The two transfer modes in HDLC are the normal response mode (NRM) and asynchronous balanced mode (ABM).
  - In the normal response mode (NRM), the station configuration is unbalanced. There is only one primary station and multiple secondary stations. A primary station can send commands whereas a secondary station can only respond.
  - In asynchronous balanced mode (ABM), the configuration is balanced. The link is point-to-point, and each station can function as a primary and a secondary (acting as peers).
  - For the HDLC protocol the following three types of stations have been defined.
    1. **Primary Station:** A primary station takes care of the data link management. The frames sent by a primary station are called commands.
    2. **Secondary Station:** A secondary station operates under the control of a primary station. The frames sent by the secondary station are called responses.
    3. **Combined Station:** A combined station can act as primary as well as secondary stations. Therefore it can send both commands and responses.

HDLC Frame:

- HDLC is a bit oriented protocol where each frame contains up to six fields. The structure varies according to the type of frame. The following Fig.4.18 Shows HDLC frame format. The fields of a HDLC frame are:

- **Flag**: It is an 8-bit sequence that marks the beginning and the end of the frame. The bit pattern of the flag is 01111110.
- **Address**: It contains the address of the receiver. If the frame is sent by the primary station, it contains the address(es) of the secondary station(s). If it is sent by the secondary station, it contains the address of the primary station. The address field may be from 1 byte to several bytes.
- **Control**: It is 1 or 2 bytes containing flow and error control information.
- **Payload**: This carries the data from the network layer. Its length may vary from one network to another.
- **FCS**: It is a 2 byte or 4 bytes frame check sequence for error detection. The standard code used is CRC (cyclic redundancy code)

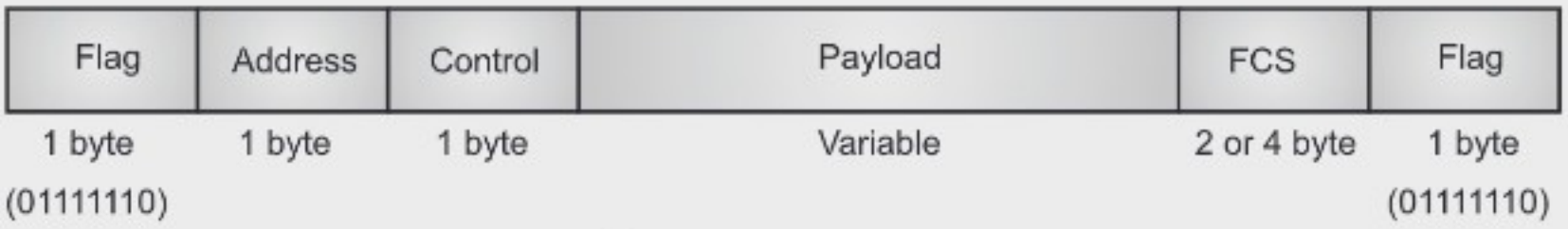


Fig. 4.18: HDLC Frame

Types of HDLC Frames

- There are three types of HDLC frames. The type of frame is determined by the control field of the frame:
  - **I-frame**: I-frames or Information frames carry user data from the network layer. They also include flow and error control information that is piggybacked on user data. The first bit of control field of I-frame is 0.
  - **S-frame**: S-frames or Supervisory frames do not contain information field. They are used for flow and error control when piggybacking is not required. The first two bits of control field of S-frame is 10.
  - **U-frame**: U-frames or Un-numbered frames are used for myriad miscellaneous functions, like link management. It may contain an information field, if required. The first two bits of control field of U-frame is 11.

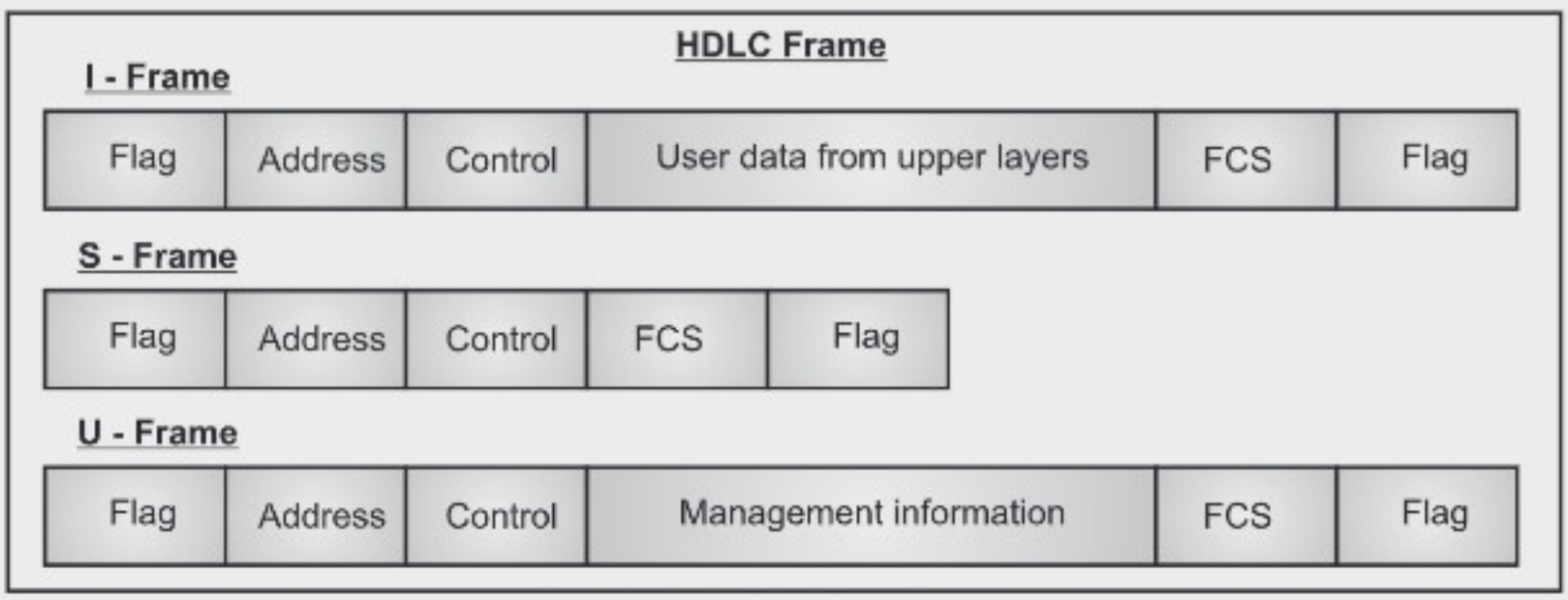


Fig. 4.19: HDLC Frame Types

4.5 SLIDING WINDOW PROTOCOLS

- The Stop and Wait ARQ offers error and flow control, but may cause big performance issues as sender always waits for acknowledgement even if it has next packet ready to send. If we have a high bandwidth connection and propagation delay is also high ,we can't use this full speed due to limitations of stop and wait.
- Sliding Window protocol handles this efficiency issue by sending more than one packet at a time with a larger sequence numbers. The term sliding window refers to the imaginary boxes to hold frames. Sliding window method is also known as windowing.

Working:

- In these protocols, the sender has a buffer called the sending window and the receiver has buffer called the receiving window.
- The size of the sending window determines the sequence number of the outbound frames. If the sequence number of the frames is an n-bit field, then the range of sequence numbers that can be assigned is 0 to 2^n –1.
- Consequently, the size of the sending window is 2^n –1. Thus in order to accommodate a sending window size of 2^n –1, n-bit sequence number is chosen.

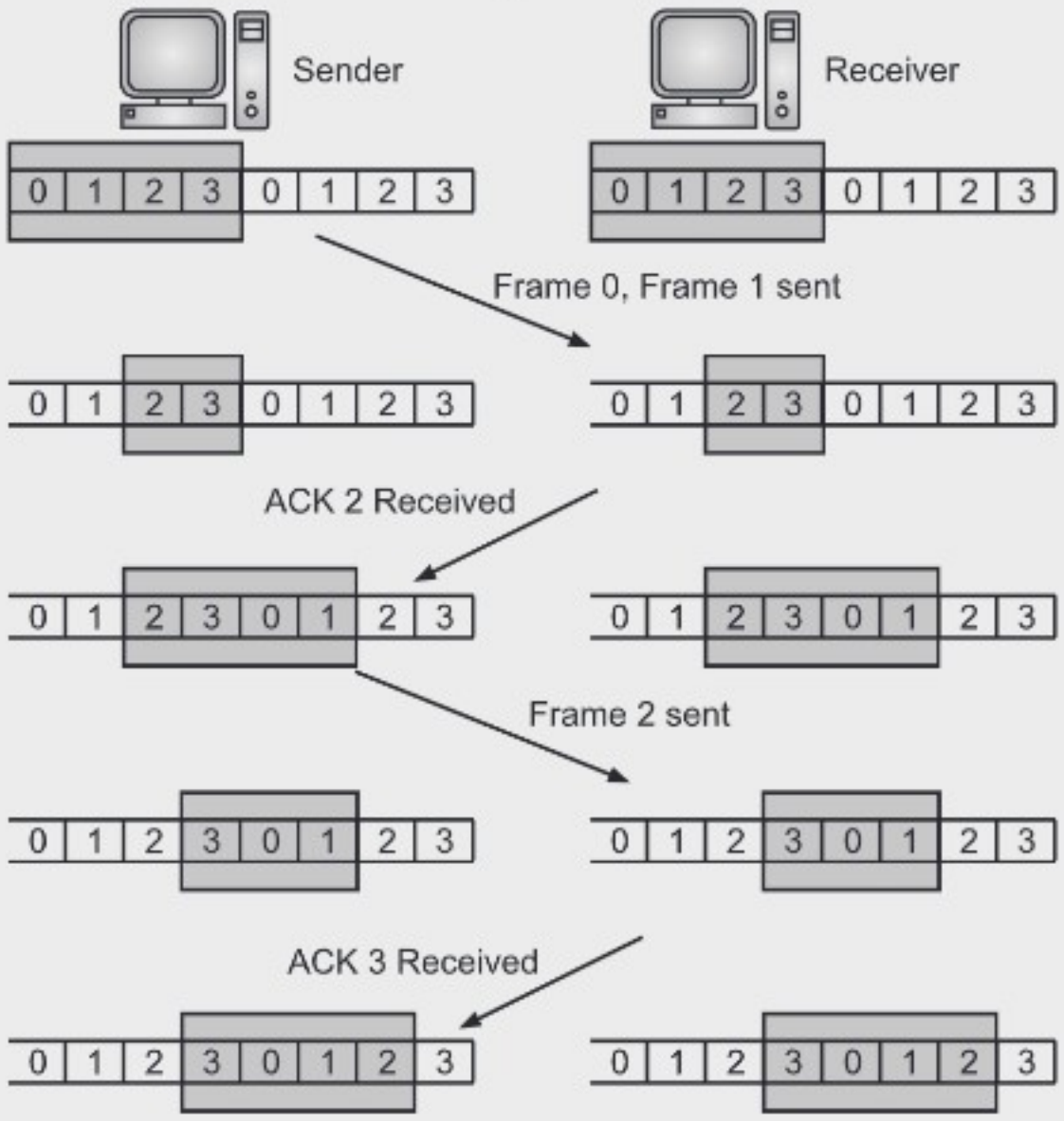


Fig. 4.20: Working of Sliding Window

- The sequence numbers are numbered as modulo-n means that they are numbered from 0 to n-1. For example, if the sending window size is 4, then the sequence numbers will be 0, 1, 2, 3, 0, 1, 2, 3, 0, 1, and so on. The number of bits in the sequence number is 2 to generate the binary sequence 00, 01, 10, 11.
- The size of the receiving window is the maximum number of frames that the receiver can accept at a time. It determines the maximum number of frames that the sender can send before receiving acknowledgment.
- For example, Suppose that we have sender window and receiver window each of size 4. So the sequence numbering of both the windows will be 0,1,2,3,0,1,2 and so on. The following figure shows the positions of the windows after sending the frames and receiving acknowledgments.
- The sliding window of sender shrinks from left when frames of data are sending. The sliding window of the sender expands to right when acknowledgments are received.
- The sliding window of the receiver shrinks from left when frames of data are received. The sliding window of the receiver expands to the right when acknowledgement is sent.

Sender Window

- At the beginning of a transmission, the sender window contains n-1 frames, and when they are sent out, the left boundary moves inward shrinking the size of the window. For example, if the size of the window is w if three frames are sent out, then the number of frames left out in the sender window is w-3.
- Once the ACK has arrived, then the sender window expands to the number which will be equal to the number of frames acknowledged by ACK.
- For example, the size of the window is 7, and if frames 0 through 4 have been sent out and no acknowledgement has arrived, then the sender window contains only two frames, i.e., 5 and 6. Now, if ACK has arrived with a number 4 which means that 0 through 3 frames have arrived undamaged and the sender window is expanded to include the next four frames. Therefore, the sender window contains six frames (5,6,7,0,1,2).

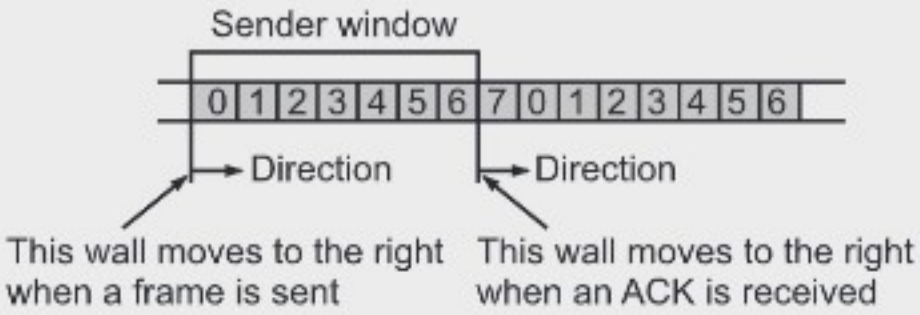


Fig. 4.21: Sender Window

Receiver Window:

- At the beginning of transmission, the receiver window does not contain n frames, but it contains n-1 spaces for frames.

- When the new frame arrives, the size of the window shrinks.
- The receiver window does not represent the number of frames received, but it represents the number of frames that can be received before an ACK is sent. For example, the size of the window is w, if three frames are received then the number of spaces available in the window is (w-3).
- Once the acknowledgement is sent, the receiver window expands by the number equal to the number of frames acknowledged.
- Suppose the size of the window is 7 means that the receiver window contains seven spaces for seven frames. If the one frame is received, then the receiver window shrinks and moving the boundary from 0 to 1. In this way, window shrinks one by one, so window now contains the six spaces. If frames from 0 through 4 have sent, then the window contains two spaces before an acknowledgement is sent.

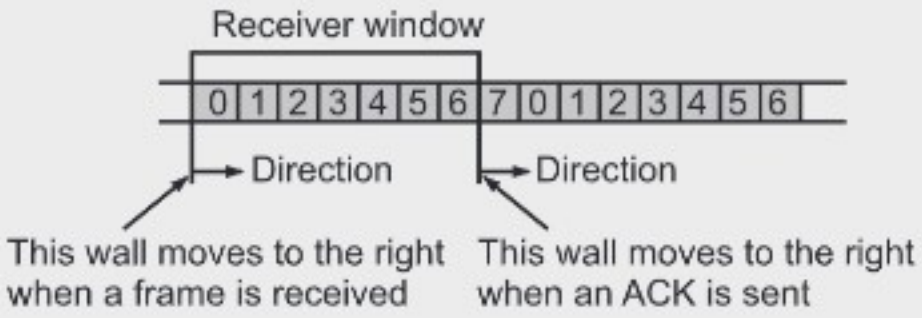


Fig. 4.22: Receiver Window

4.5.1 1-bit Sliding Window Protocols

1. In one – bit sliding window protocol, the size of the window is 1. So the sender transmits a frame, waits for its acknowledgment, then transmits the next frame. Thus it uses the concept of stop and waits for the protocol. This protocol provides for full – duplex communications.
2. Problem with Stop-And-Wait protocol is that it is very inefficient. At any one moment, only in frame is in transition. The sender will have to wait at least one round trip time before sending next. The waiting can be long for a slow network such as satellite link.
3. In this protocol, the sender fetches the packet, builds a frame and sends it. The receiver window checks to see if it is a duplicate frame. If the frame is arrived which was expected, it is accepted and the receiver window is slide up.
4. The acknowledgment field contains the number of the last frame received without error. If it matches with the frame. The sender is trying to send then the frame is stored in the buffer and next frame is send. If they do not match, it will resend the same frame.
5. Let us see the simple example. A is trying to send frame 0 to computer B and B is trying to send its frame 0 to A. A sends frame to B and A's timeout interval is too short. So, A may continuously send identical frames to B.

6. When the first valid frame arrives at computer B, it will be accepted. All other frames will be rejected because, B is expecting a frame with sequence number 1 and not 0. Now B is waiting for an acknowledgment of 0 and will not send any more frames.
7. This situation arises if both sides simultaneously send an initial packet. Here, duplicate frames are delivered even though there is no transmission error.
8. Diagrammatically, it can be represented as follows:
   - Show normal operation.
   - A and B starts simultaneously, so there are duplicates. The format is (sequential acknowledgment, packet number). An asterisk indicates where a network layer accepts a packet.

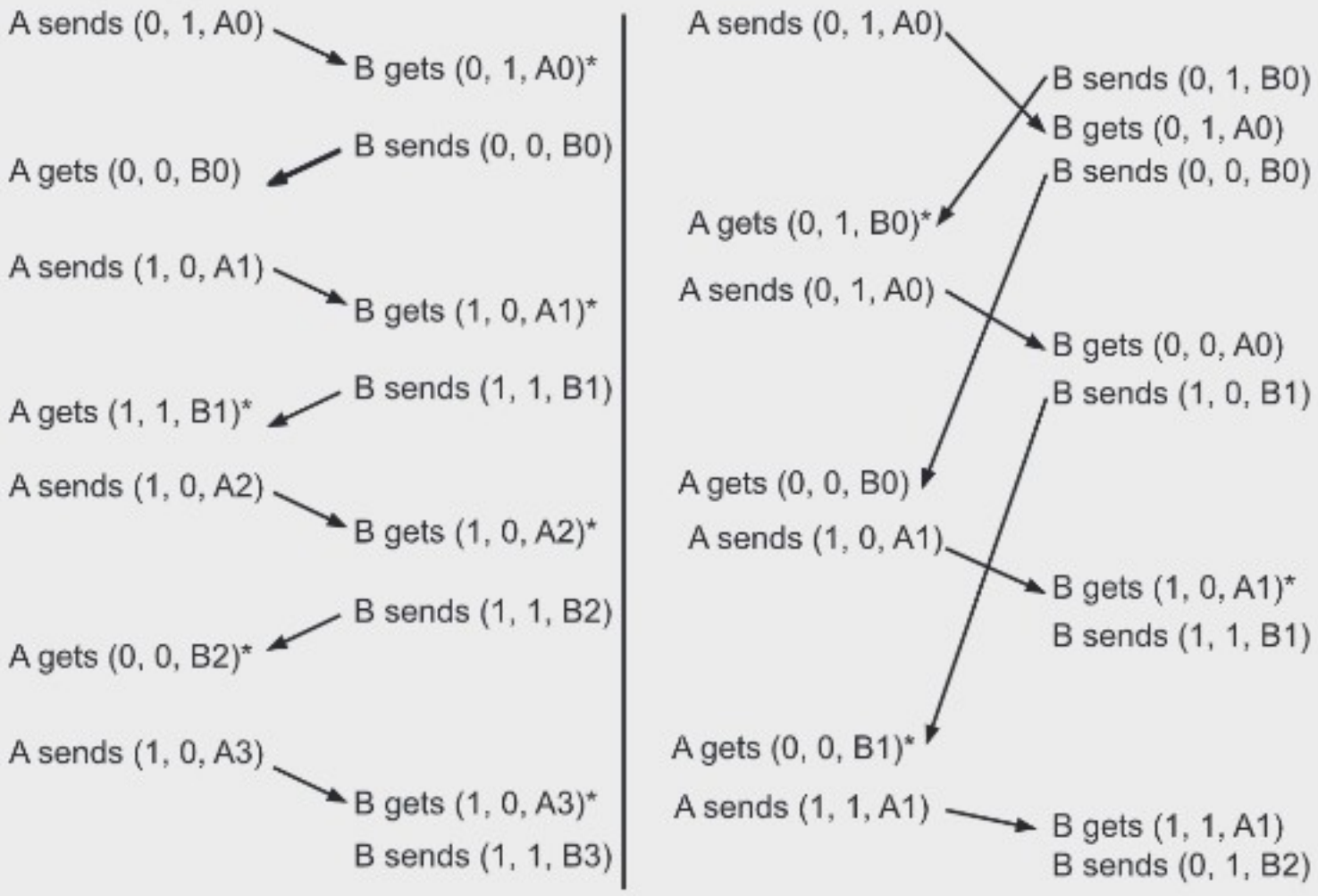


Fig. 4.23: Representation of 1- bit Sliding Window Protocol

Advantages:

1. Multiple packets can be transmit without waiting for acknowledgements
2. Piggybacking can be beneficial using full-duplex lines.

Disadvantages:

1. No limit of the size or sequence numbers that can be required in this protocol.
2. The bandwidth may be wasted in some special situations.

4.5.2 Piggybacking

- In full – duplex transmission, the data flow occurs in both directions. To achieve full – duplex communication, both the communication is considered as a pair of simplex communication. Each link comprises a forward channel for sending data and a

reverse channel for sending acknowledgments. However, in the above arrangement, traffic load doubles for each data unit that is transmitted. Half of all data transmission comprise of transmission of acknowledgments.

- So, a solution that provides better utilization of bandwidth is piggybacking. Here, sending of acknowledgment is delayed until the next data frame is available for transmission. The acknowledgment is then hooked onto the outgoing data frame. The data frame consists of an *ack* field. The size of the *ack* field is only a few bits, while an acknowledgment frame comprises of several bytes. Thus, a substantial gain is obtained in reducing bandwidth requirement.
- In reliable full - duplex data transmission, the technique of hooking up acknowledgments onto outgoing data frames is called piggybacking.

Working Principle:

- Suppose that there are two communication stations X and Y. The data frames transmitted have an acknowledgment field, *ack* field that is of a few bits length. Additionally, there are frames for sending acknowledgments, ACK frames. The purpose is to minimize the ACK frames.
- The three principles governing piggybacking when the station X wants to communicate with station Y are:
  1. If station X has both data and acknowledgment to send, it sends a data frame with the *ack* field containing the sequence number of the frame to be acknowledged.
  2. If station X has only an acknowledgment to send, it waits for a finite period of time to see whether a data frame is available to be sent. If a data frame becomes available, then it piggybacks the acknowledgment with it. Otherwise, it sends an ACK frame.
  3. If station X has only a data frame to send, it adds the last acknowledgment with it. The station Y discards all duplicate acknowledgments. Alternatively, station X may send the data frame with the *ack* field containing a bit combination denoting no acknowledgment.
- The following Fig. 4.24 illustrates the three scenario-

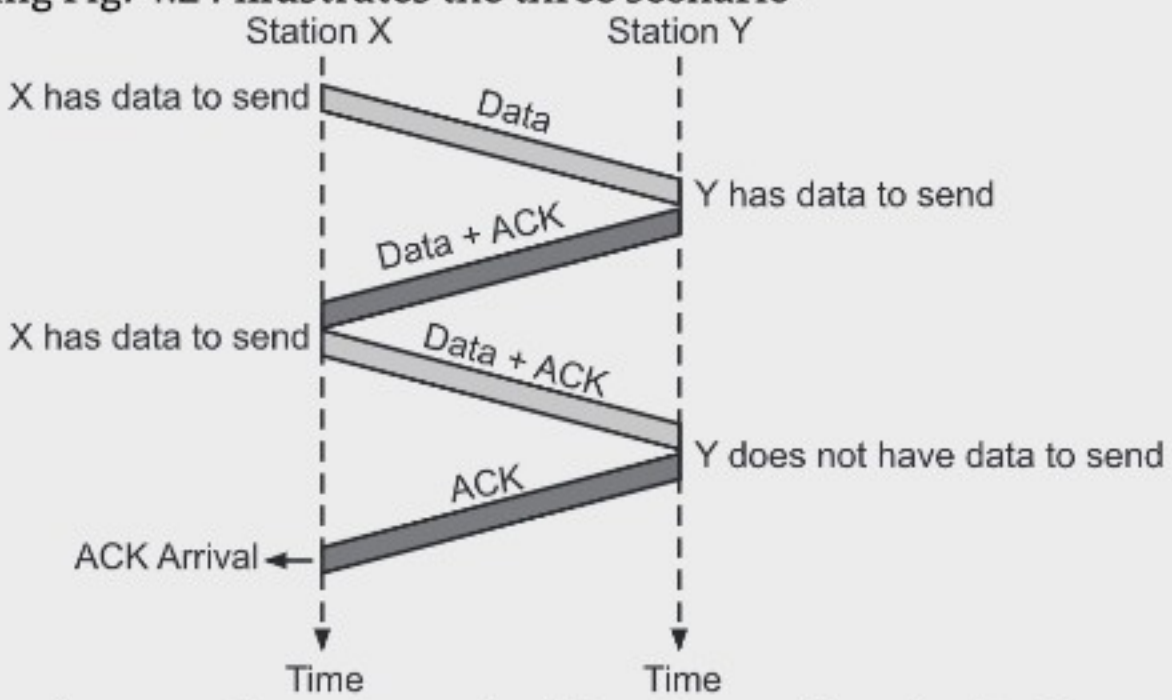


Fig. 4.24: Shows three principles of governing piggybacking

Advantages of Piggybacking:

1. A better use of available channel bandwidth.
2. The acknowledgment field is only a few bits whereas the entire acknowledgment frame would consist of many bits because of header, checksum etc.
3. Fewer frames sent means fewer received reducing the traffic and requires fewer buffers in the receiver.

Disadvantages of Piggybacking:

1. The main problem with piggybacking is how long the sender should wait for a packet onto which the acknowledgment is sent. If it waits longer than the senders timeout, the frame will be retransmitted.
2. Actually piggybacking is used for better channel utilization, here due to retransmission bandwidth is wasted.

4.5.3 Pipelining – Go-Back-N and Selective Repeat

- Pipelining is a process of sending multiple data frames serially without waiting for the previous acknowledgement.
- This technique is beneficial when the amount of data to be transferred is very large, and we send the data by dividing them into various parts.
- These data parts can be pipelined and sent to the receiver over the channel. In pipelining, we do not wait for the acknowledgement of sent data frames. We keep on sending the data frames continuously without bothering about the acknowledgements.
- Hence, pipelining ensures the efficient and better utilization of network resources. It also enhances the speed of delivery of data frames, ensuring the timely transmission of data.
- Two basic approaches are available for dealing with errors in the presence of pipelining i.e. Go-Back-N, and Selective Repeat

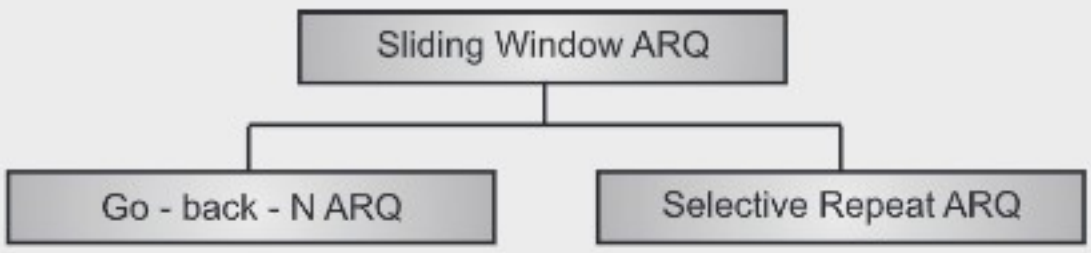


Fig. 4.25: Types of Sliding Window ARQ using Pipelining

1. **Go-Back-N ARQ:**

- Go-Back-N ARQ makes efficient use of a connection than Stop-and-wait ARQ. Go – Back – N ARQ provides for sending multiple frames before receiving the acknowledgment for the first frame.
- In this protocol, the sending process continues to send a number of frames specified by a window size even without receiving an acknowledgement (ACK) packet from the receiver.

- Unlike waiting for an acknowledgement for each packet in stop-and-wait ARQ, the connection is still being utilized as packets are being sent. In other words, during the time that would otherwise be spent waiting, more packets are being sent.
- It is a special case of the general sliding window protocol with the transmit window size of N and receive window size of 1. It can transmit N frames to the peer before requiring an ACK.
- The receiver process keeps track of the sequence number of the next frame it expects to receive, and sends that number with every ACK it sends.
- The receiver will discard any frame that does not have the exact sequence number it expects (either a duplicate frame it already acknowledged, or an out-of-order frame it expects to receive later) and will resend an ACK for the last correct in-order frame.
- Once the sender has sent all of the frames in its window, it will detect that all of the frames since the first lost frame are outstanding, and will go back to the sequence number of the last ACK it received from the receiver process and fill its window starting with that frame and continue the process over again.
- Consider the figure given below. Suppose sender window size of 4. Now the sender has sent the packets 0, 1, 2 and 3. After acknowledging the packets 0 and 1, receiver is now expecting packet 2 and sender window has also slided to further transmit the packets 4 and 5.
- Now suppose the packet 2 is lost in the network, Receiver will discard all the packets which sender has transmitted after packet 2 as it is expecting sequence number of 2. On the sender side for every packet send there is a time out timer which will expire for packet number 2.
- Now from the last transmitted packet number 5 sender will go back to the packet number 2 in the current window and transmit all the packets till packet number 5. That's why it is called Go Back N. Go back means sender has to go back N places from the last transmitted packet in the unacknowledged window and not from the point where the packet is lost.

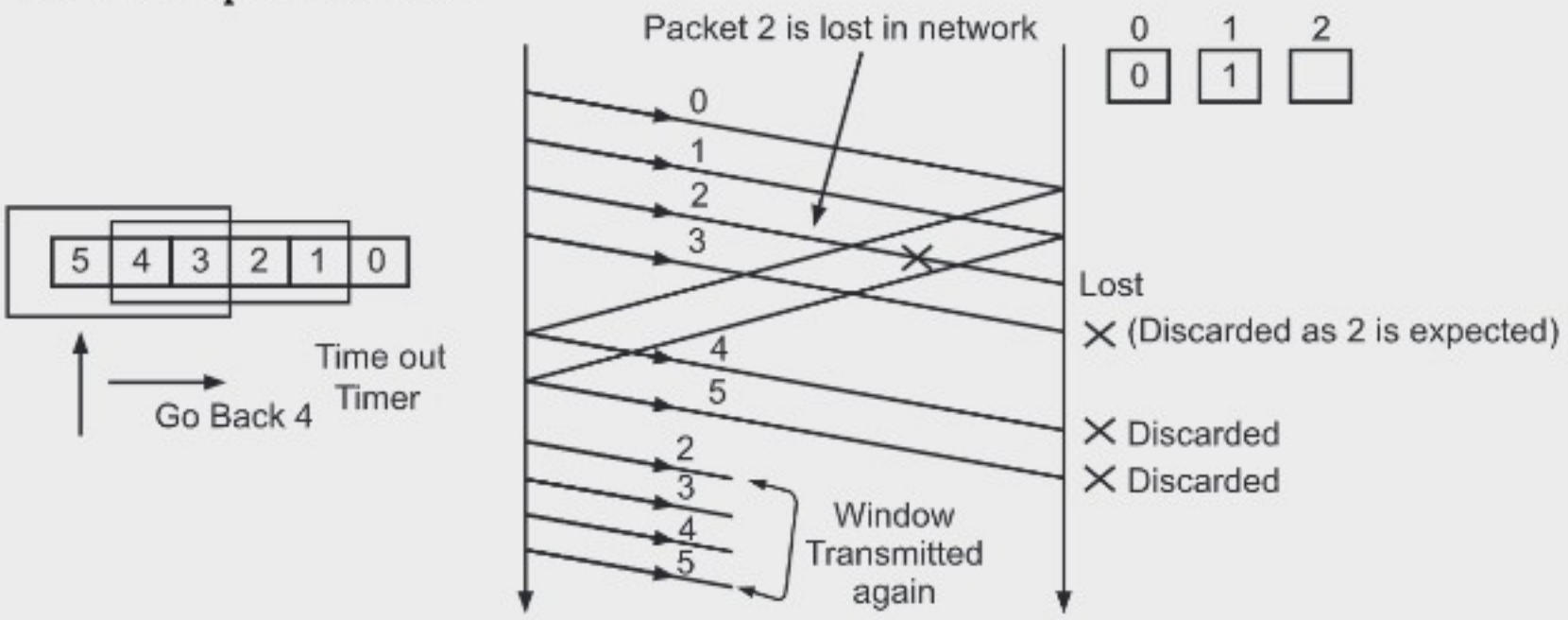


Fig. 4.26: Working of Go-Back-N protocol

Design of Go-Back-N protocol:

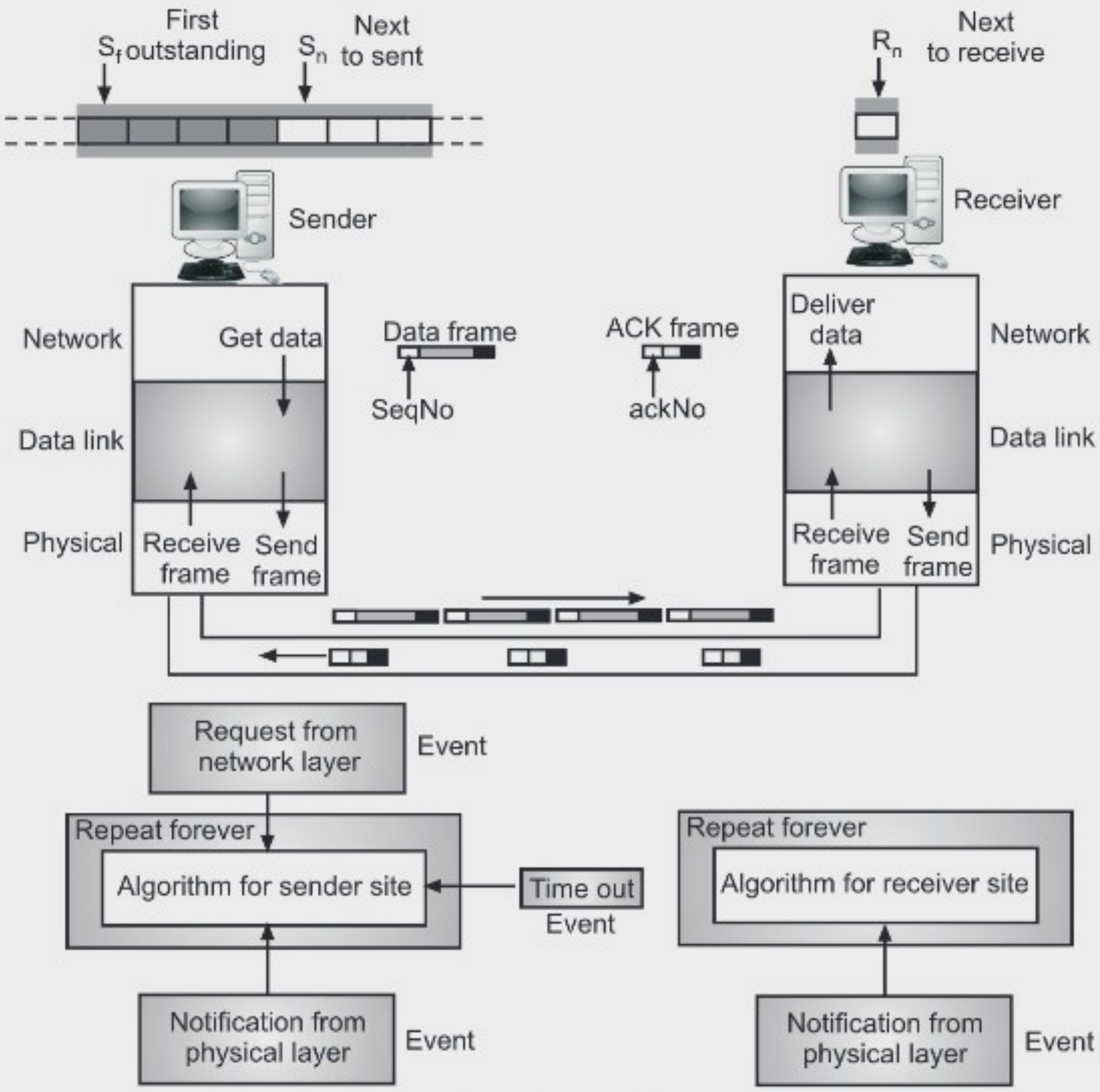
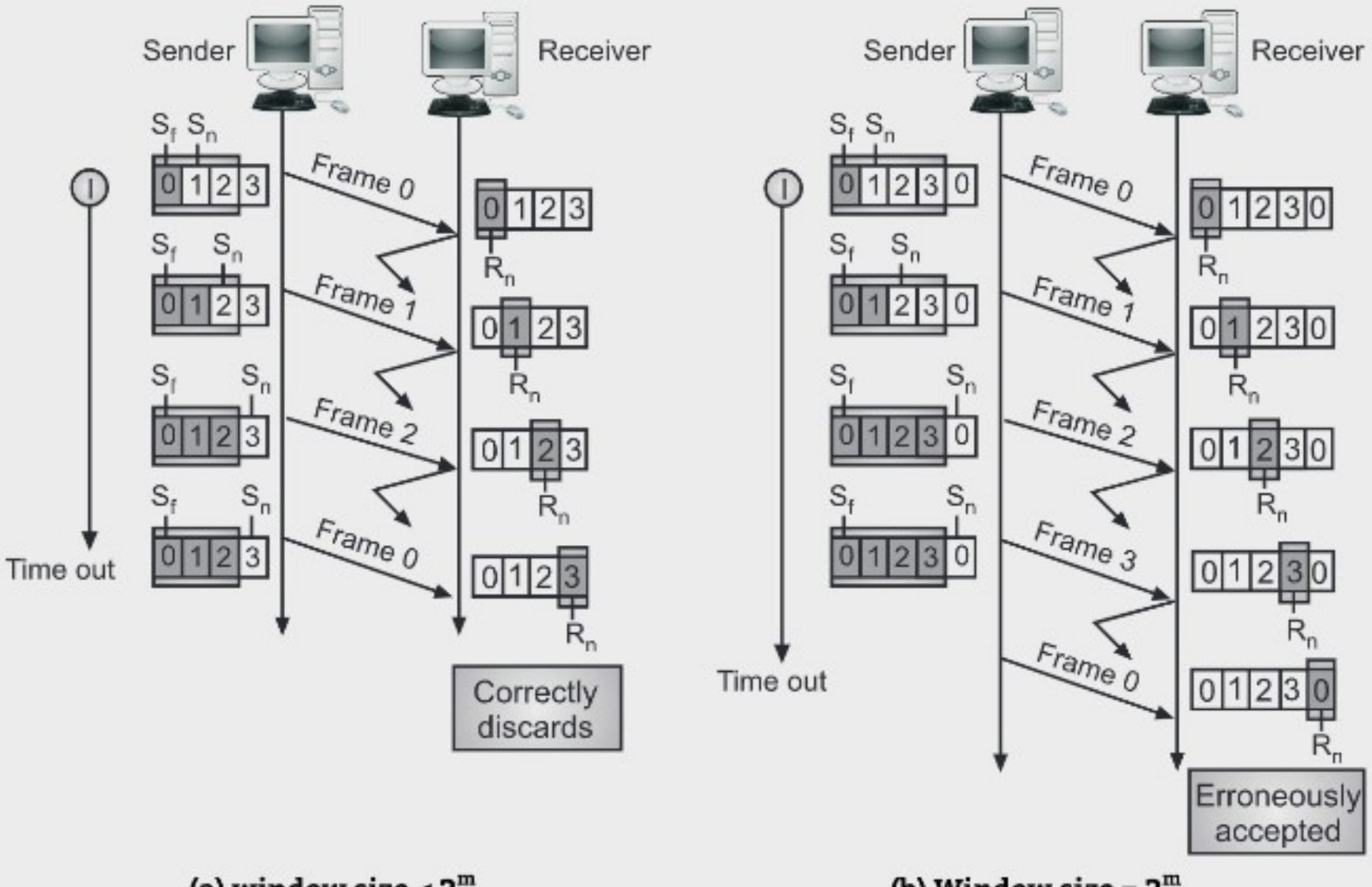


Fig. 4.27: Design of Go-Back-N protocol

- Figure 4.27 shows the design for Go-Back-N protocol. As we can see, multiple frames can be transit in the forward direction, and multiple acknowledgments in the reverse direction. The idea is similar to Stop-and-Wait ARQ; the difference is that the send window allows us to have as many frames in transition as there are slots in the send window.

Send Window Size:

- The size of the send window must be less than 2^m. As an example, we choose m =2, which means the size of the window can be 2^m- 1, or 3. The following compares a window size of 3 against a window size of 4. If the size of the window is 3 (less than 22) and all three acknowledgments are lost, the frame 0 timer expires and all three frames are re-sent. The receiver is now expecting frame 3, not frame 0, so the duplicate frame is correctly discarded.



(a) window size < 2^m **(b) Window size = 2^m**

Fig. 4.28: Comparison between window size < 2^m and Window size = 2^m

Advantages of Go-Back N :

1. The sender can send many frames at a time.
2. Timer can be set for a group of frames.
3. Only one ACK can acknowledge one or more frames.
4. Efficiency is more.
5. Waiting time is low.
6. We can alter the size of the sender window.

Disadvantages of Go-Back N:

1. Buffer requirement is more.
2. Transmitter needs to store the last N packets.
3. Scheme is inefficient when round-trip delay large and data transmission rate is high.
4. If NACK is lost, a long time is wasted until re-transmission of all packets (until another NACK is sent).

2. Selective Repeat ARQ:

- In Go-Back N method results in sending frames multiple times – if any frame was lost or damaged, or the ACK acknowledging them was lost or damaged, then that

frame and all following frames in the send window (even if they were received without error) will be re-sent. To avoid this, Selective Repeat ARQ can be used.

- Selective Repeat ARQ protocol supports sending of multiple frames before receiving the acknowledgment for the first frame. However, here only the erroneous or lost frames are retransmitted, while the good frames are received and buffered.

Working:

- The Selective Repeat Protocol also uses two windows: a send window and a receive window.
- Sender window size is always same as receiver window size.
- If n bits are available for sequence numbers, then- Sender window size = Receiver window size = $2^n/2 = 2^{n-1}$. This is to avoid packets being recognized incorrectly. If the windows size is greater than half the sequence number space, then if an ACK is lost, the sender may send new packets that the receiver believes are retransmissions.
- Selective Repeat protocol provides for sending multiple frames depending upon the availability of frames in the sending window, even if it does not receive acknowledgement for any frame in the interim. The maximum number of frames that can be sent depends upon the size of the sending window.
- Receiver acknowledges each frame independently. As receiver receives a new frame from the sender, it sends its acknowledgement.
- The receiver records the sequence number of the earliest incorrect or un-received frame. It then fills the receiving window with the subsequent frames that it has received. It sends the sequence number of the missing frame along with every acknowledgement frame.
- The sender continues to send frames that are in its sending window. Once, it has sent all the frames in the window, it retransmits the frame whose sequence number is given by the acknowledgements. It then continues sending the other frames.
- If receiver receives a frame that is corrupted, then it does not silently discard that frame. Receiver handles the situation efficiently by sending a negative acknowledgement (NACK). Negative acknowledgement allows early retransmission of the corrupted frame. It also avoids waiting for the time out timer to expire at the sender side to retransmit the frame.
- If receiver receives a frame whose sequence number is not what the receiver expects, then it does not discard that frame rather accepts it and keeps it in its window.

Design:

- The design in this case is to some extent similar to the Go Back-N, but more complicated, as shown in the following figure.

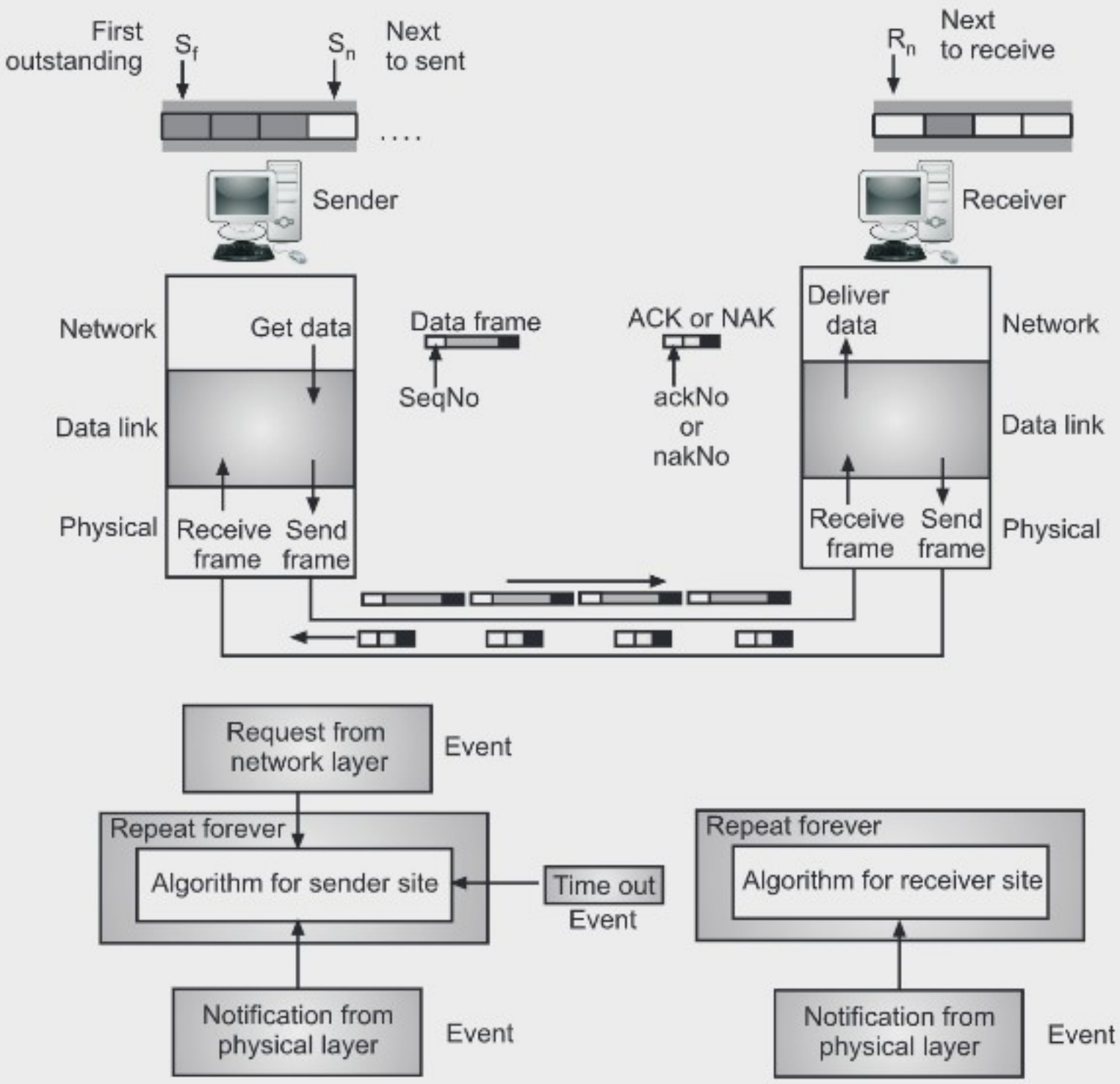


Fig. 4.29: Design of Selective Repeat

- This is the most efficient among the ARQ schemes, but the sender must be more complex so that it can send out-of-order frames. The receiver also must have storage space to store the post NAK frames and processing power to reinsert frames in proper sequence.

Table 4.2: Comparison between Go-Bach-N, Stop and Wait, Selective Repeat

Sr. No.	Protocol	Go-Back-N	Stop and Wait	Selective Repeat
1.	Bandwidth utilization	Medium	Low	High
2.	Maximum sender Size Window	2^m-1	N.A.	2^(m-1)
3.	Maximum receiver Size Window	1	N.A.	2^(m-1)

4.	Pipelining	Implemented	Not implemented	Implemented
5.	Out of order Frames	Discarded	Discarded	Accepted
6.	Cumulative ACK	Applicable	N.A.	Applicable
7.	NAK	N.A.	N.A.	Applicable

4.6 RANDOM ACCESS PROTOCOLS

- As we have seen already, according to transmission technology the networks are divided into two major categories, i.e. Point-to-point connections and Broadcast channels.
- In point-to-point network dedicated links are reserved for communication, whereas in broadcast network all stations share a single communication channel.
- The main problem with the broadcast network is that who will get to use the channel when there is a competition for it. Because if more than one station, simultaneously going to access the channel accident (collision) of data packet will occurs. Both time and bandwidth will be wasted.
- Broadcast channels are sometimes called as multi-access channels or random access channels.
- As we know Data link layer is divided into two sub layers i.e. Logical Link Control (LLC) and Medium Access Control (MAC) Layer.
- MAC layer provides addressing and channel access control mechanisms that make it possible for several stations to communicate within a multiple access network that incorporates a shared medium, for example, Ethernet.
- Many formal protocols have been devised to handle access to a shared link. We categorize them into three groups.

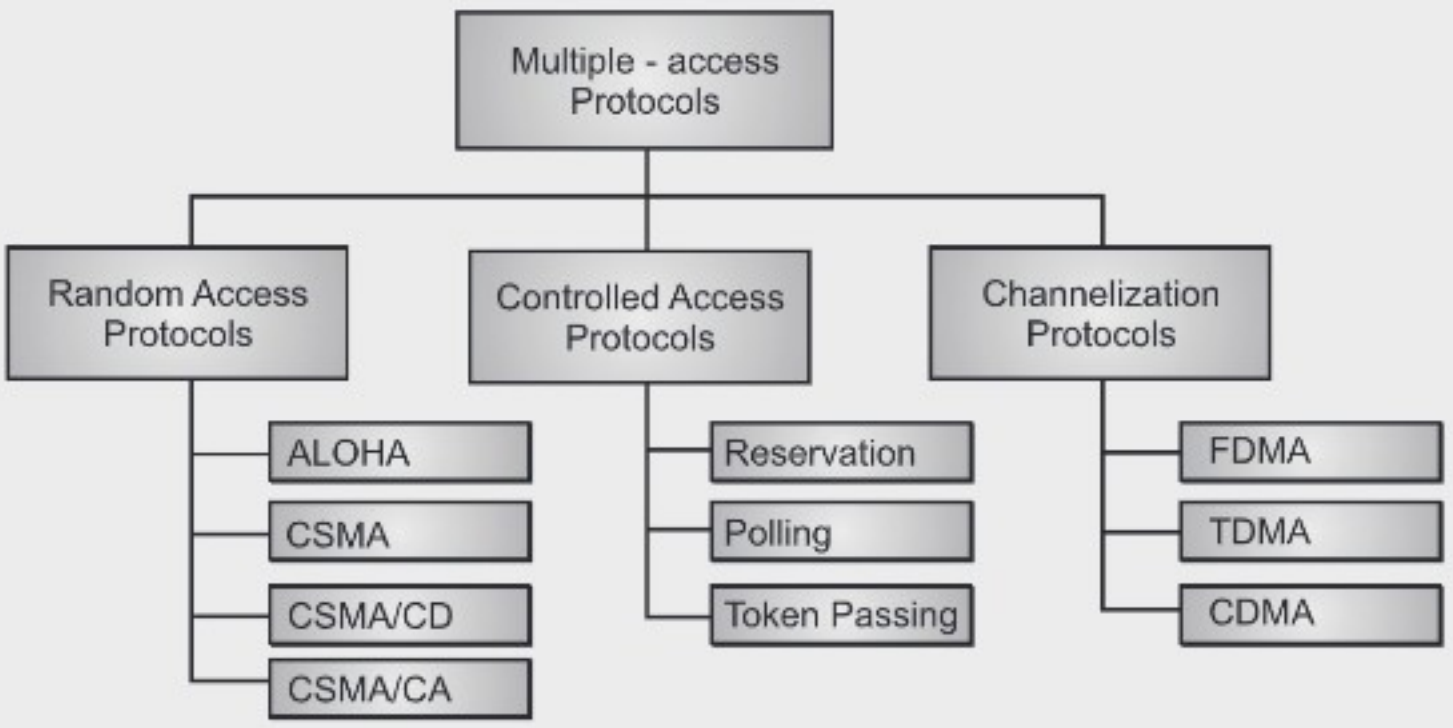


Fig. 4.30: Categories of Multiple Access Protocol

- Protocols belonging to each group are shown in the Fig. 4.30
  1. **Random Access Protocols:** In these type of protocols any station can transmit at any time. Use of the channel is not controlled by any station.
  2. **Controlled Access Protocols:** In controlled access some sort of mechanism is used to decide which station can transmit.
  3. **Channelization:** In channelization, the available channel bandwidth is shared either in frequency, time or code.

Concept of Random Access Protocols:

- In random access or contention method, each station in the network has equal right.
- No station is superior to other station. No station permits, or does not permit another station to send. All can have direct access to the medium through which the information or data flows. And that individual station is not controlled by any other station.
- At any instance of time, stations which want to transmit data uses a procedure defined by protocol, and decide whether to transmit or not.
- This decision depends upon whether medium is free or busy.
- Random access protocols has two features:
  1. There is no scheduled time for a station to transmit. Transmission is random among the stations.
  2. No rules specify which station should send next. Stations compete with one another to access the medium. So these protocols also called contention method.
- Even though, if more stations tried to send frames then there may be a conflict called collision occurs or the frames may be destroyed or modified.
- To avoid this collision, modification etc., we need a procedure which handles the situation properly. And it will help us to get answers of few questions like:
  1. When station can access the medium?
  2. If medium is busy, what station can do?
  3. If collision occurs, what station can do?
  4. How station gets information about the success and failure of a transmission?
- To answer these types of questions, we have evolution of random access methods. These are shown in Fig. 4.31.

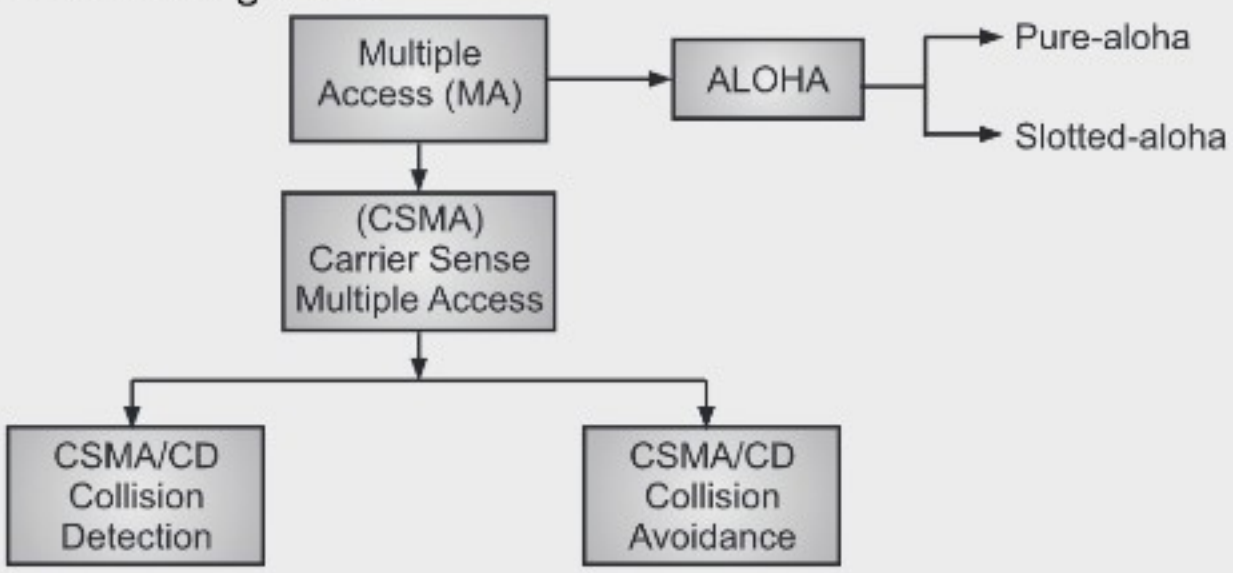


Fig. 4.31: Evolution of Random Access Methods

- In this case, Multiple Access (MA) is a simple procedure called ALOHA. This method was improved with the addition of procedure on the basis of sense the medium before transmitting. This is called CSMA i.e. carrier sense multiple access which has two parallel methods i.e. CSMA/CD and CSMA/CA.
- CSMA/CA is for collision avoidance which defines a procedure to avoid the collision. CSMA/CD is for collision detection which defines to be followed if collision is detected.

4.6.1 ALOHA

- ALOHA is a system for coordinating and arbitrating access to a shared communication Networks channel.
- ALOHA was developed in the 1970s by Norman Abramson and his colleagues at the University of Hawaii to solve the problem of channel allocation.
- ALOHA was designed for a wireless LAN, but it can be used on any shared medium.
- The medium is shared between the stations. When a station sends data , another station may attempt to send data same time. It is obvious that the data from the two stations collide and destroyed.
- There are two types of ALOHA protocols i.e., Pure ALOHA and Slotted ALOHA as discussed in following sections.

4.6.1.1 Pure ALOHA (W-18)

- The original ALOHA protocol is called pure ALOHA.
- Concept of ALOHA is very simple, each station sends a frame whenever it has frame to send. Since there is only one channel to share, there is possibility of collisions between frames from different stations.
- Fig. 4.32 shows an example of frame collisions in pure ALOHA.
- In Fig. 4.32 four stations are shown. Every station sends a frames on shared medium. Some of these frames collide because multiple frames are in contention for the shared channel. Only two frames, frame 1.1 and frame 2.2 survive. All other frames are destroyed.
- In pure ALOHA, whenever any station transmits a frame, it expects the acknowledgement from the receiver. If acknowledgement is not received within specified time, the station assumes that the frame (or acknowledgement) has been destroyed.
- If the frame is destroyed because of collision the station waits for a random amount of time and sends it again. This waiting time must be random otherwise same frames will collide again and again.
- Therefore pure ALOHA dictates that when time-out period passes, each station must wait for a random amount of time before resending its frame. This randomness will help avoid more collisions.

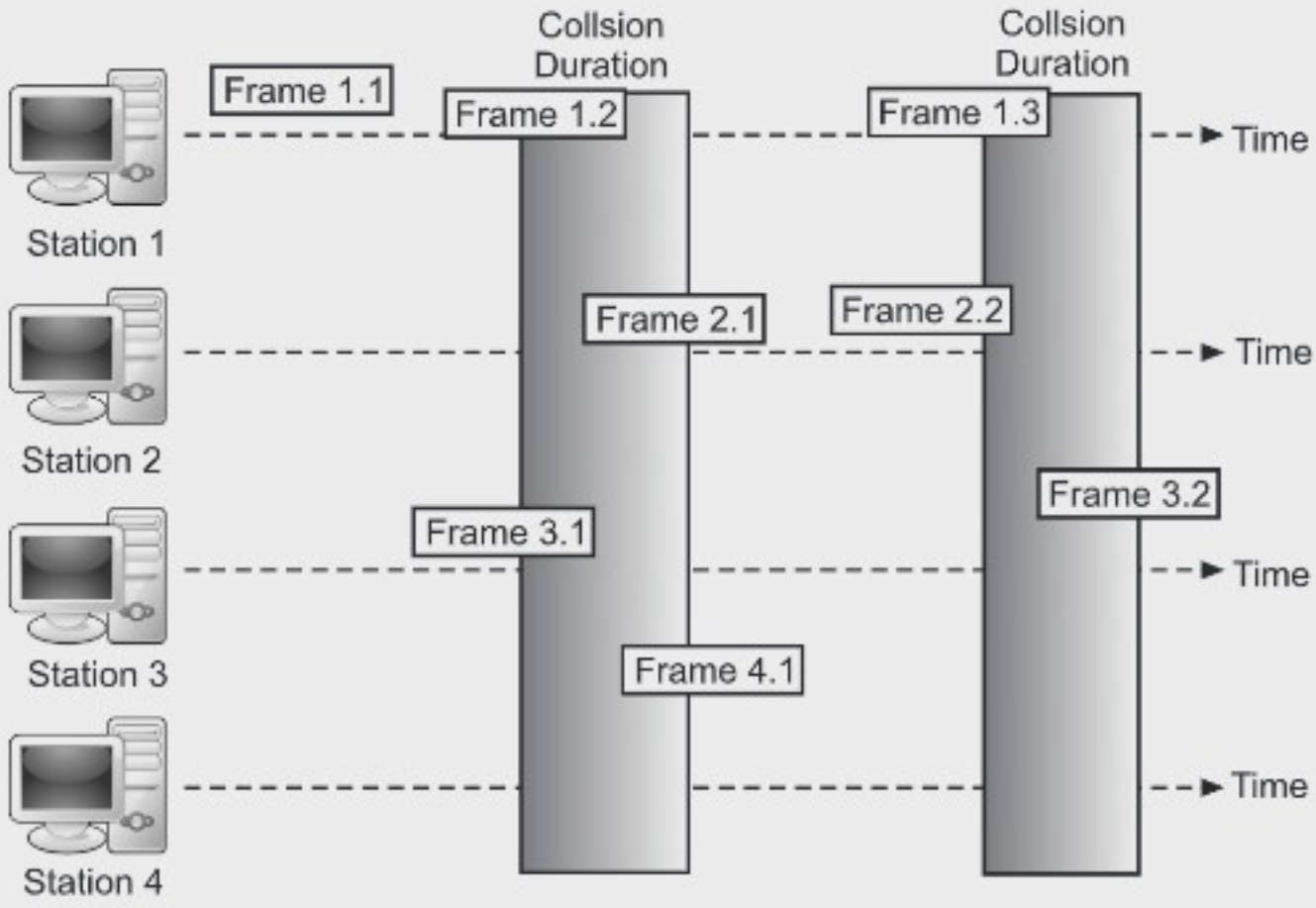


Fig. 4.32: Frames in Pure ALOHA

- The pure ALOHA protocol has second method to prevent congesting the channel with retransmissions. It is shown in Fig. 4.33.

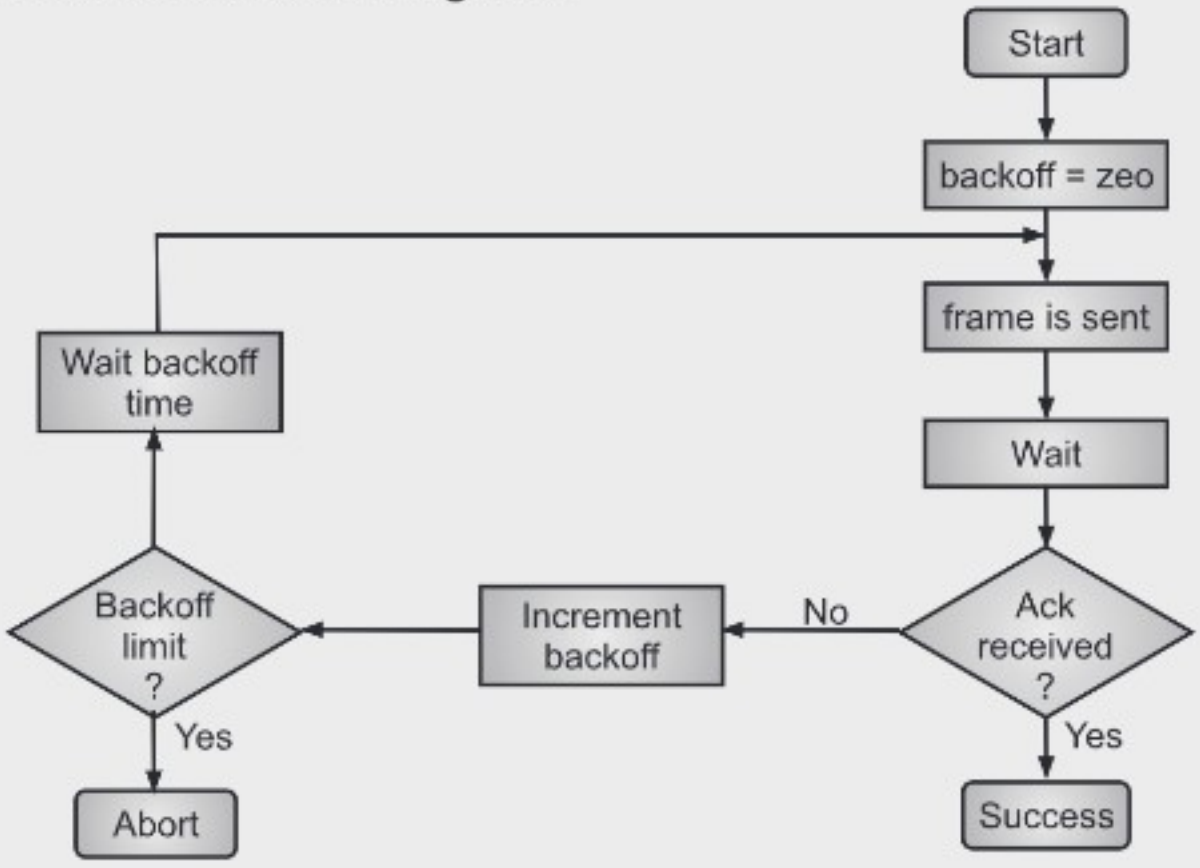


Fig. 4.33: ALOHA Protocol Procedure

- A node or station sends the frame. Then wait for a period of time which is 2 times the maximum propagation delay.
- If the acknowledgement is received, the transmission is successful. If the acknowledgement is not given then station has to use a backoff strategy and send the packet again. After several tries, if it is not happen then procedure is aborted.

- **Vulnerable Time:** Vulnerable time is a time in which there is possibility of collision. It is calculated as,

$$\text{Pure ALOHA vulnerable time} = 2 \times T_{fr}$$

- **Throughput:** Let G be the average number of frames generated by the system during one frame transmission time. Then average number of successful transmission for pure ALOHA is $S = G \times e^{-2G}$. The maximum throughput of pure ALOHA is 0.184 i.e. not more than 18.4 %.

Example 3: A pure ALOHA network transmits 200-bit frames on a shared channel of 200 kbps. What is the throughput if the system (all stations together) produces:

(a) 1000 frames per second, (b) 500 frames per second and (c) 250 frames per second.

Solution:

The frame transmission time is 200/200 kbps or 1 ms.

(a) If the system creates 1000 frames per second, this is 1 frame per millisecond. The load is 1. In this case $S = G \times e^{-2G}$ or S = 0.135 (13.5 percent). This means that the throughput is 1000 × 0.135 = 135 frames. Only 135 frames out of 1000 will probably survive.

(b) If the system creates 500 frames per second, this is (1/2) frame per millisecond. The load is (112). In this case $S = G \times e^{-2G}$ or S = 0.184 (18.4 percent). This means that the throughput is 500 × 0. 184 = 92 and that only 92 frames out of 500 will probably survive. Note that this is the maximum throughput case, percentagewise.

(c) If the system creates 250 frames per second, this is (1/4) frame per millisecond. The load is (1/4). In this case $S = G \times e^{-2G}$ or S = 0.152 (15.2 percent). This means that the throughput is 250 × 0.152 = 38. Only 38 frames out of 250 will probably survive.

4.6.1.2 Slotted ALOHA (S-19)

- An improvement to the original ALOHA protocol was "Slotted ALOHA", which introduced discrete timeslots and increased the maximum throughput.
- Slotted ALOHA was invented to improve the efficiency of pure ALOHA as chances of collision in pure ALOHA are very high.
- In slotted ALOHA, the time of the shared channel is divided into discrete intervals called slots.
- The stations can send a frame only at the beginning of the synchronized time slot and only one frame is sent in each slot.
- In slotted ALOHA, if any station is not able to place the frame onto the channel at the beginning of the slot i.e. it misses the time slot then the station has to wait until the beginning of the next time slot.
- In slotted ALOHA, there is still a possibility of collision if two stations try to send at the beginning of the same time slot as shown in Fig. 4.34.

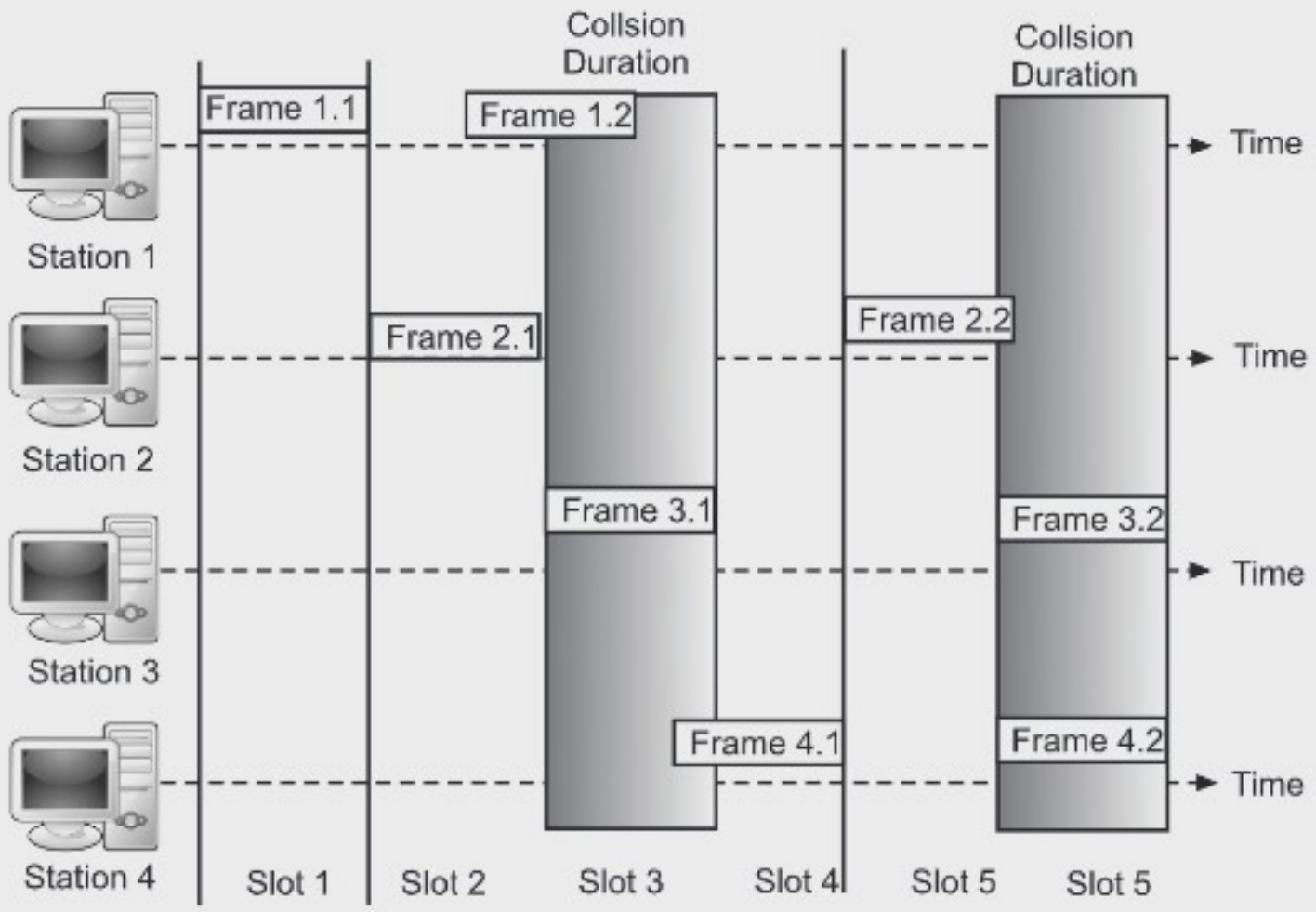


Fig. 4.34: Frames in Slotted ALOHA

- Slotted ALOHA still has an edge over pure ALOHA as chances of collision are reduced to one-half. Slotted ALOHA requires global time synchronization.
- **Vulnerable Time:** It reduces the vulnerable period from 2T to T frames and improves efficiency by reducing the probability of collision.

Slotted ALOHA vulnerable time = T fr

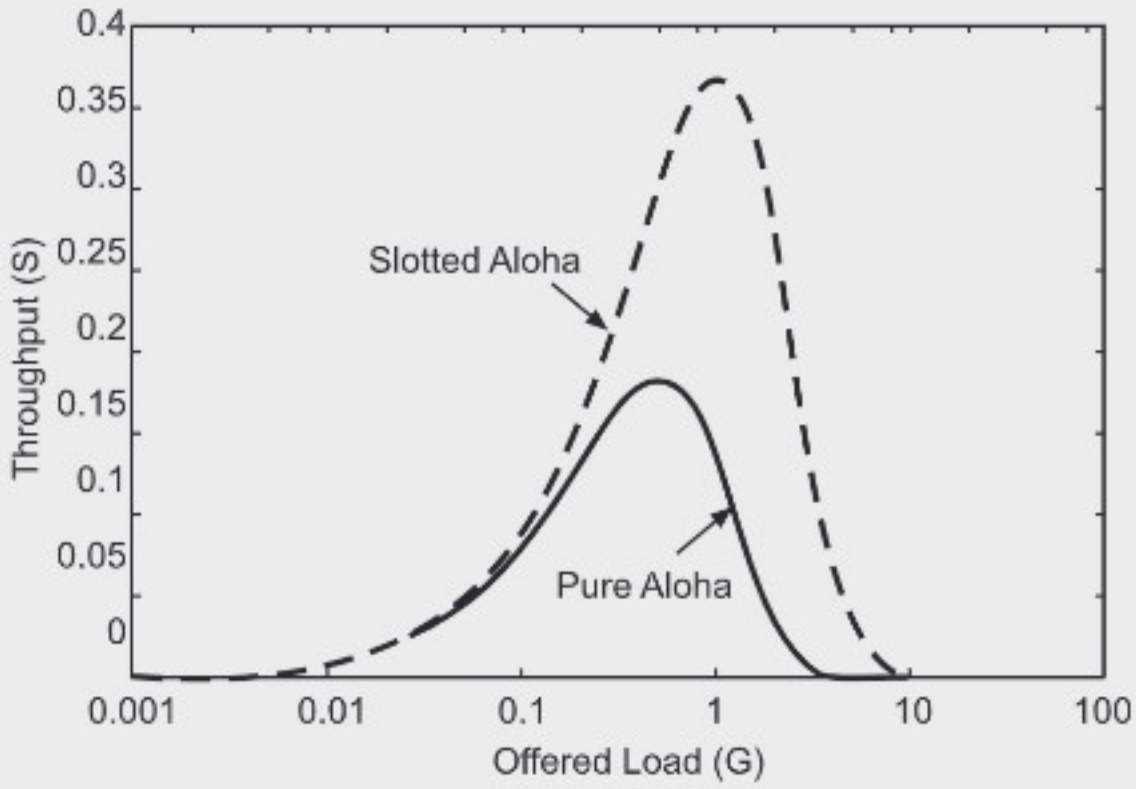


Fig. 4.35: Throughput of Pure and Slotted ALOHA

- **Throughput:**
  Slotted ALOHA is $S = G \times e^{-G}$.
- The maximum throughput of slotted ALOHA is 0.37 i.e. not more than 37 %.

Example 4: A slotted ALOHA network transmists 200-bit frames using a shared channel with a 200-kbps bandwidth. Find the throughput if the system (all stations together) produces:

(a) 1000 frames per second,

(b) 500 frames per second, and

(c) 250 frames per second.

Solution: This solution is similar to the previous example except that the network is using slotted ALOHA instead of pure ALOHA. The frame transmission time is 200/200 kpbs or 1 ms.

(a) In this case G is 1. So $S = G \times e^{-G}$ or S = 0.368 (36.8 percent). This means that the throughput is 1000 × 0.0368 = 368 frames. Only 368 out of 1000 frames will probably survive. Note that this is the maximum throughput case, percentagewise.

(b) Here G is 1/2. In this case $S = G \times e^{-G}$ or S = 0.303 (30.3 per cent). This means that the throughput is 500 × 0.0303 = 151. Only 151 frames out of 500 will probably survive.

(c) Now G is 1/4. In this case $S = G \times e^{-G}$ or S = 0.195 (19.5 percent). This means that the throughtput is 250 × 0.195 = 49. Only 49 frames out of 250 will probably survive.

4.6.2 CSMA

- The poor efficiency of the ALOHA scheme can be attributed to the fact that a node start transmission without paying any attention to what others are doing.
- In situations where propagation delay of the signal between two nodes is small compared to the transmission time of a packet, all other nodes will know very quickly when a node starts transmission. This observation is the basis of the Carrier Sense Multiple Access (CSMA) protocol.
- In this scheme, a node having data to transmit first listens to the medium to check whether another transmission is in progress or not. The node starts sending only when the channel is free, that is there is no carrier. That is why the scheme is also known as listen-before talk.
- CSMA is a network access method used on shared network topologies such as Ethernet to control access to the network.
- Devices attached to the network cable listen (carrier sense) before transmitting. If the channel is in use, devices wait before transmitting. MA (Multiple Access) indicates

that many devices can connect to and share the same network. All devices have equal access to use the network when it is clear.

- Even though devices attempt to sense whether the network is in use, there is a good chance that two stations will attempt to access it at the same time. On large networks, the transmission time between one end of the cable and another is enough that one station may access the cable even though another has already just accessed it.

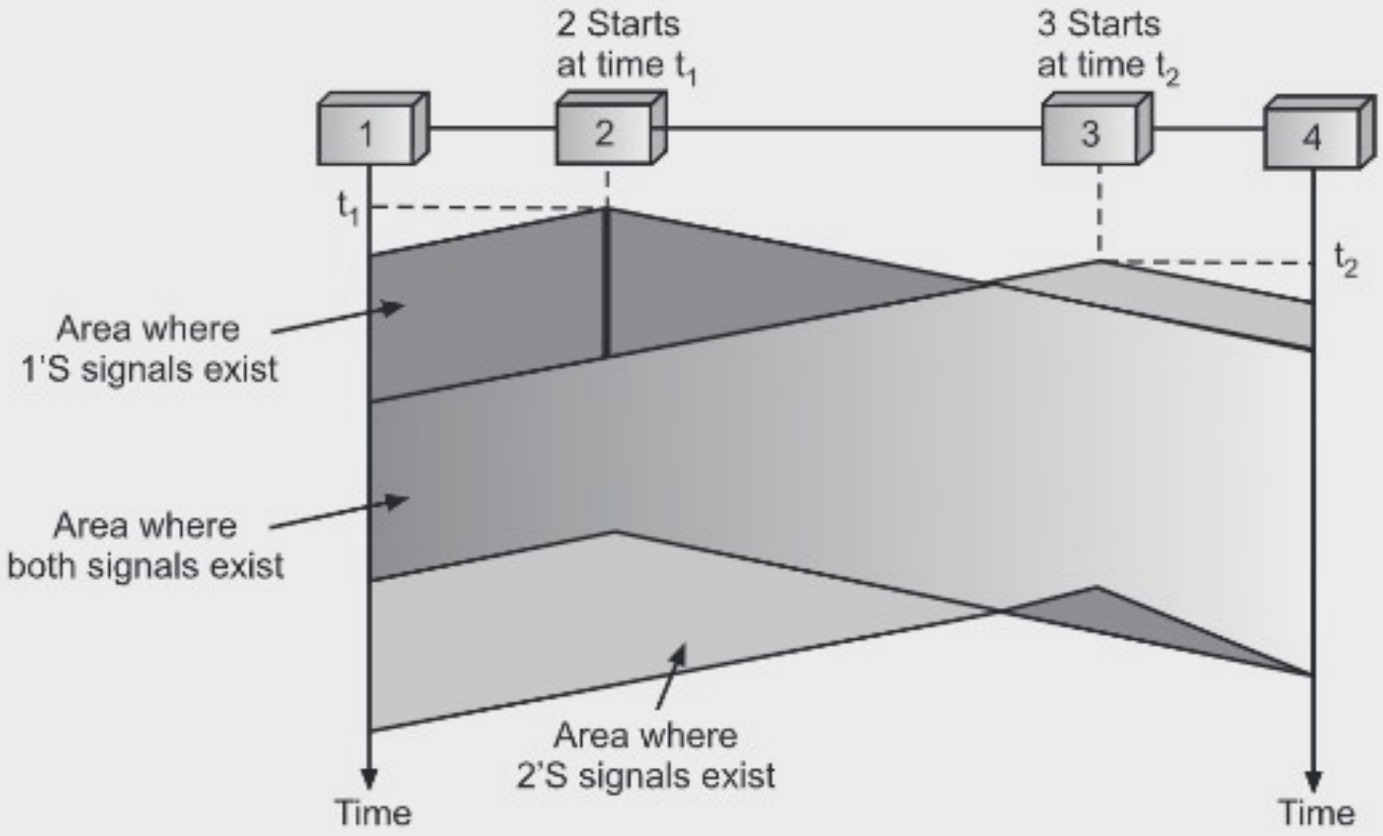


Fig. 4.36: Time/Space Model of the Collision in CSMA

- The chances of collision still exist because of propagation delay. The frame transmitted by one station takes some time to reach other stations. In the meantime, other stations may sense the channel to be idle and transmit their frames. This results in the collision, as shown in Fig. 4.36.
- In CSMA, Carrier Sense (CS) means that whenever a device wants to send a packet over the network media, it first listens to the network media to see whether anyone else is already sending a packet. Multiple Access (MA) means that nothing prevents two or more devices from trying to send a message at the same time. Sure, each device listens before sending.

Vulnerable Time:

- The vulnerable time for CSMA is the propagation time Tp_1, needed for a signal to propagate from one end of the medium to the other. When a station sends a frame, and any other station tries to send, collision occurs. But if the first bit of the frame reaches the end of the medium, other stations will already have heard the bit and will stop ourselves from sending.

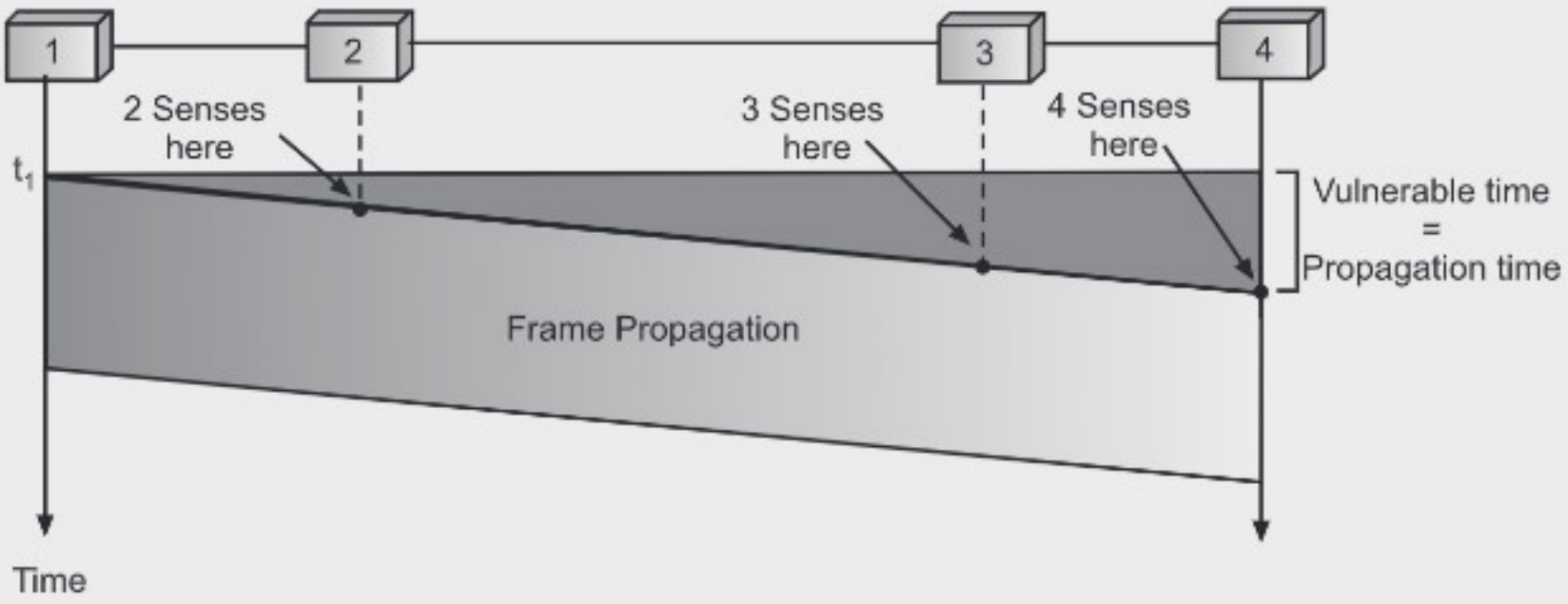


Fig. 4.37: Vulnerable time in CSMA

Persistence Methods:

- If channel is free, definitely station will transmit data. But if channel is busy, what should a station do? Three different protocols are invented for this.
- There are three different type of CSMA protocols i.e., 1-persistent CSMA, Non-persistent CSMA and P-persistent CSMA as shown in Fig. 4.38.

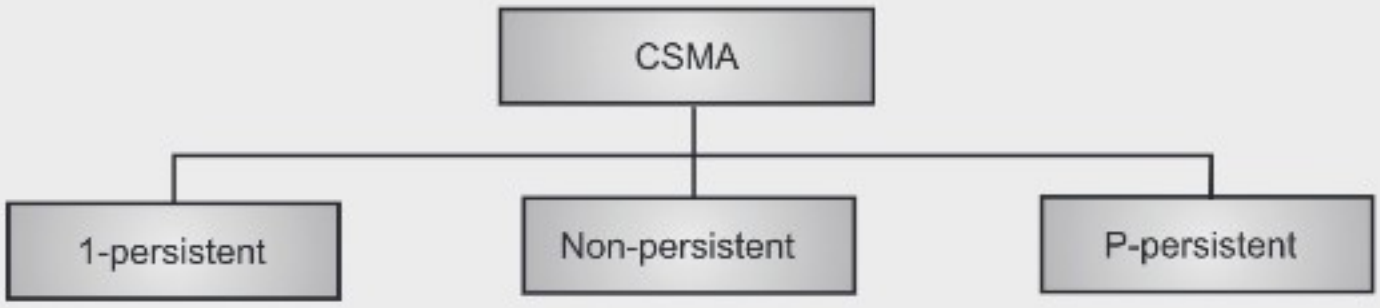


Fig. 4.38: Types of CSMA

4.6.2.1 1-persistent CSMA

- This method is very simple and straightforward.
- In 1-persistent CSMA method, station that wants to transmit data continuously senses the channel to check whether the channel is idle or busy. If the channel is busy, the station waits until it becomes idle.
- When the station detects an idle-channel, it immediately transmits the frame with probability 1. Hence, it is called 1-persistent CSMA.
- This method has the highest chance of collision because two or more stations may find channel to be idle at the same time and transmit their frames.
- When the collision occurs, the stations wait a random amount of time and start all over again.
- The 1-persistent CSMA is used in CSMA/CD systems including Ethernet.

Drawback of 1-persistent CSMA:

- The propagation delay time greatly affects this protocol. Let us suppose, just after the station 1 begins its transmission, station 2 also became ready to send its data and senses the channel.
- If the station 1 signal has not yet reached station 2, station 2 will sense the channel to be idle and will begin its transmission. This will result in collision.

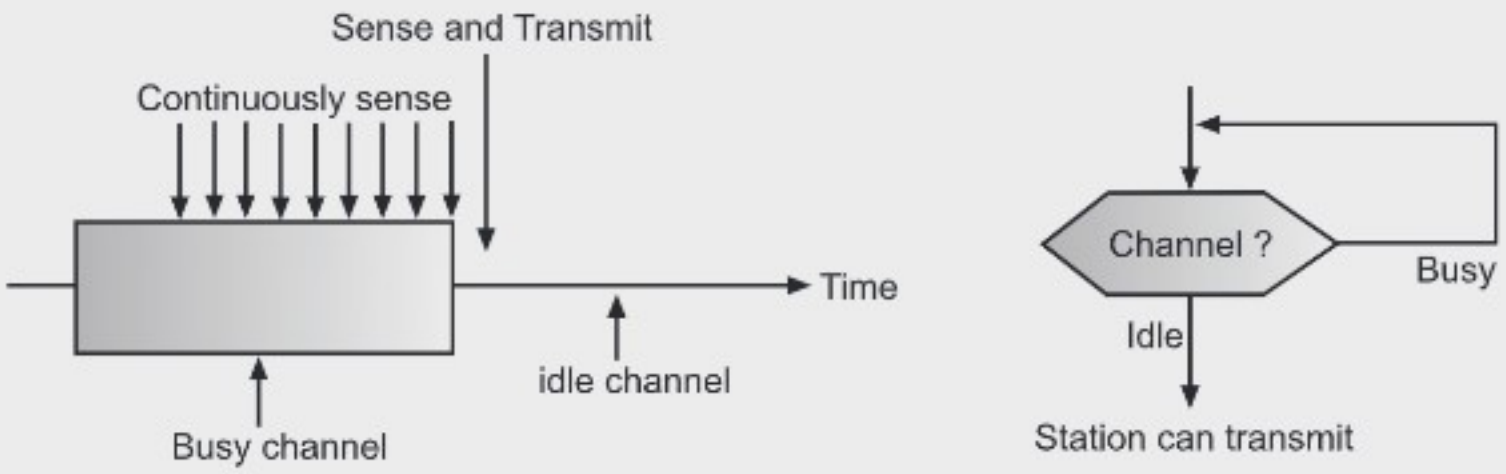


Fig. 4.39: 1-persistent CSMA

- Even if propagation delay time is zero, collision will still occur. If two stations became ready in the middle of third station's transmission, both stations will wait until the transmission of first station ends and then both will begin their transmission exactly simultaneously. This will also result in collision.

4.6.2.2 Non-persistent CSMA

- In non persistent CSMA, a station that has a frame to send senses the channel. If the channel is idle, it sends immediately. If the channel is busy, it waits for a random amount of time and then senses the channel again.

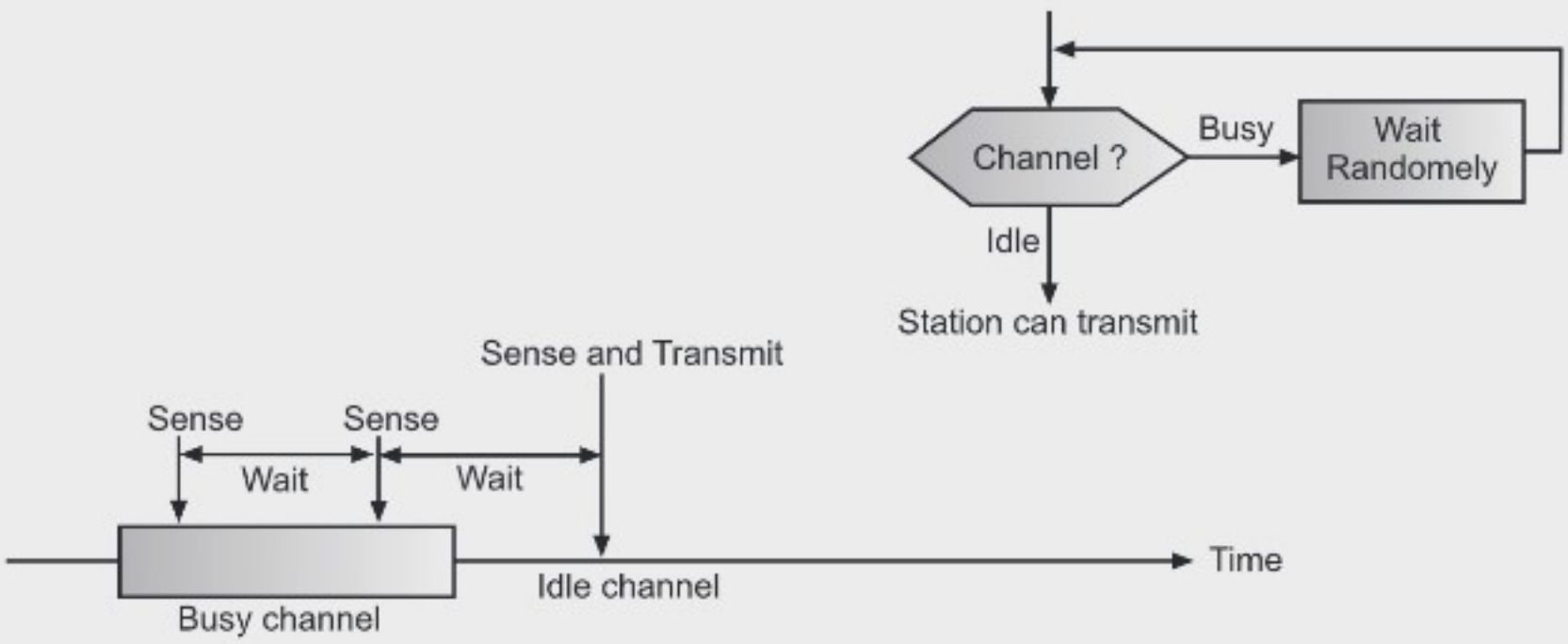


Fig. 4.40: Non-persistent CSMA

- In non-persistent CSMA, the station does not continuously sense the channel for the purpose of capturing it when it detects the end of previous transmission.

Advantage of Non-persistent CSMA: **(S-18)**

1. It reduces the chance of collision because the stations wait a random amount of time.
2. It is unlikely that two or more stations will wait for same amount of time and will retransmit at the same time.

Disadvantage of Non-persistent CSMA:

1. It reduces the efficiency of network because the channel remains idle when there may be stations with frames to send.
2. This is due to the fact that the stations wait a random amount of time after the collision.

4.6.2.3 P-persistent CSMA

- This method is used when channel has time slots such that the time slot duration is equal to or greater than the maximum propagation delay time.
- Whenever a station becomes ready to send, it senses the channel. If channel is busy, station waits until next slot. If channel is idle, it transmits with a probability p. With the probability q=1-p, the station then waits for the beginning of the next time slot.

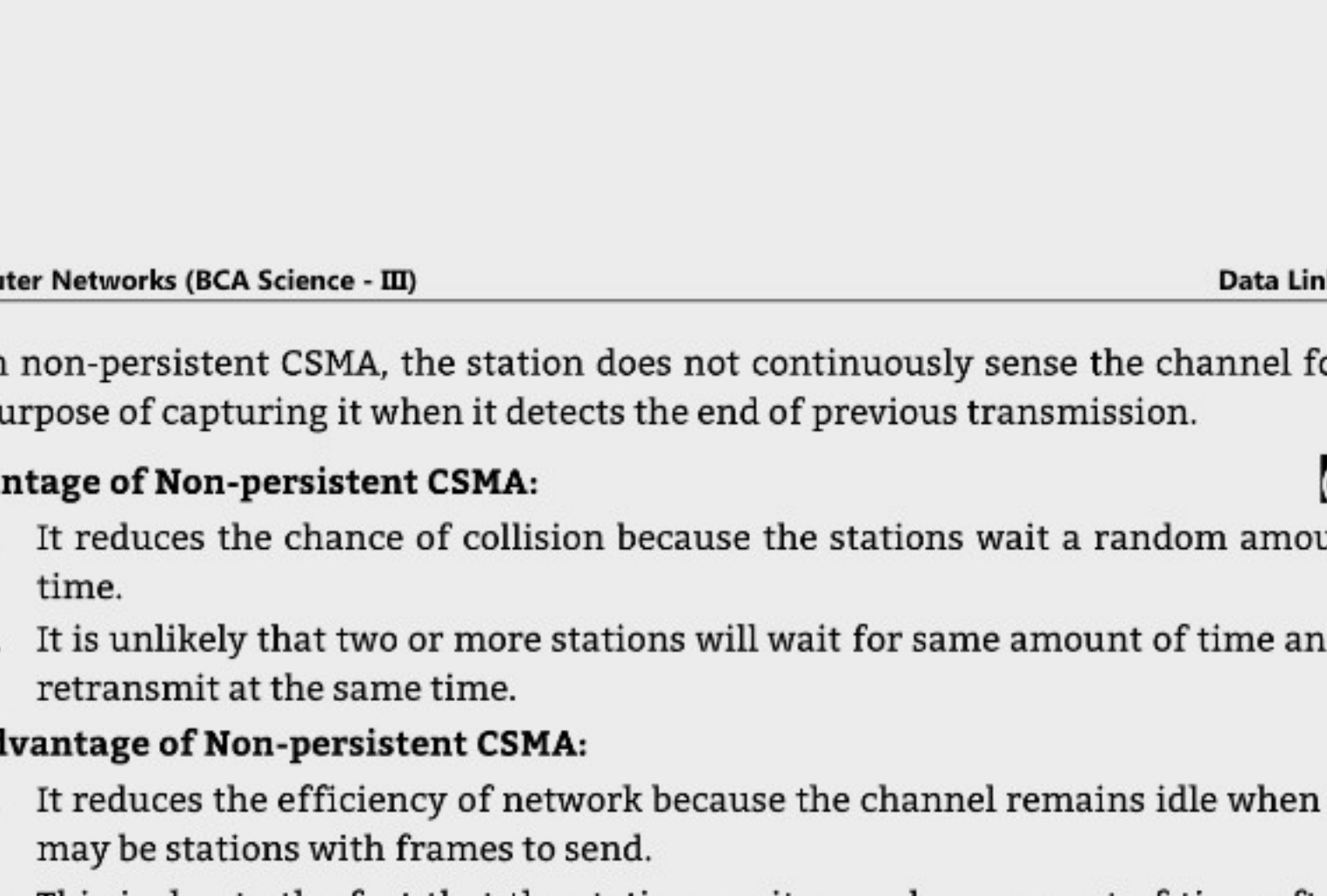


Fig. 4.41: P-persistent CSMA

- If the next slot is also idle, it either transmits or waits again with probabilities p and q. This process is repeated till either frame has been transmitted or another station has begun transmitting.
- In case of the transmission by another station, the station acts as a collision has occurred and it waits a random amount of time and starts again.
- Advantage of p-persistent CSMA is it reduces the chance of collision and improves the efficiency of the network.
- P-persistent CSMA is used in CSMA/CA systems including Wi-Fi and other packet radio systems.
- The efficiency of CSMA scheme depends on the propagation delay, which is represented by a parameter a, as defined below:

  a = Propagation delay / Packet transmission time
- It may be noted that smaller the value of propagation delay, lower is the vulnerable period and higher is the efficiency.

4.6.3 CSMA/CD (W-18)

- CSMA/CD stands for Carrier Sense Multiple Access with Collision Detection. Collision detection means that after a device sends a packet, it listens carefully to see whether the packet crashes into another packet.
- CSMA/CD protocol can be considered as a refinement over the CSMA scheme. It has evolved to overcome one glaring inefficiency of CSMA. In CSMA scheme, when two packets collide the channel remains unutilized for the entire duration of transmission time of both the packets. If the propagation time is small (which is usually the case) compared to the packet transmission time, wasted channel capacity can be considerable.
- This wastage of channel capacity can be reduced if the nodes continue to monitor the channel while transmitting a packet and immediately stop transmission when collision is detected. This refined scheme is known as CSMA/CD or Listen-While-Talk.
- On top of the CSMA, the following rules are added to convert it into CSMA/CD:
  1. If a collision is detected during transmission of a packet, the node immediately stops transmission and it transmits jamming signal for a brief duration to ensure that all stations know that collision has occurred.
  2. After transmitting the jamming signal, the node waits for a random amount of time and then transmission is resumed.
- The random delay ensures that the nodes, which were involved in the collision, are not likely to have a collision at the time of retransmissions. To achieve stability in the back off scheme, a technique known as binary exponential back off is used. A node

will attempt to transmit repeatedly in the face of repeated collisions, but after each collision, the mean value of the random delay is doubled.

- Therefore the CSMA/CD method consists of alternating transmission period and collisions with idle periods when none of the stations is transmitting.

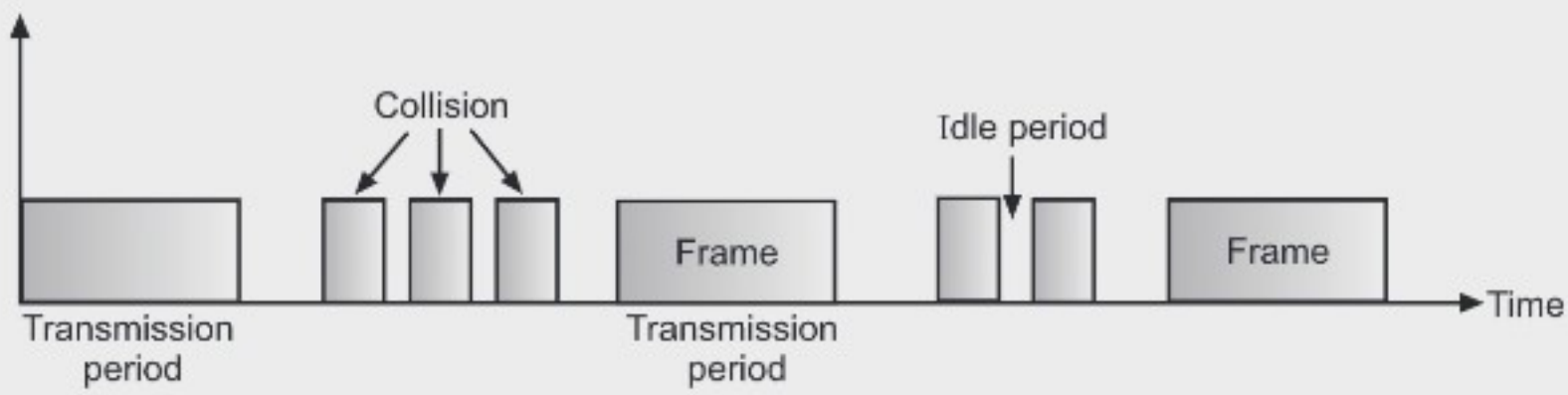


Fig. 4.42: CSMA/CD with Three States

- The entire scheme of CSMA/CD is described in the Fig. 4.43 and 4.44.

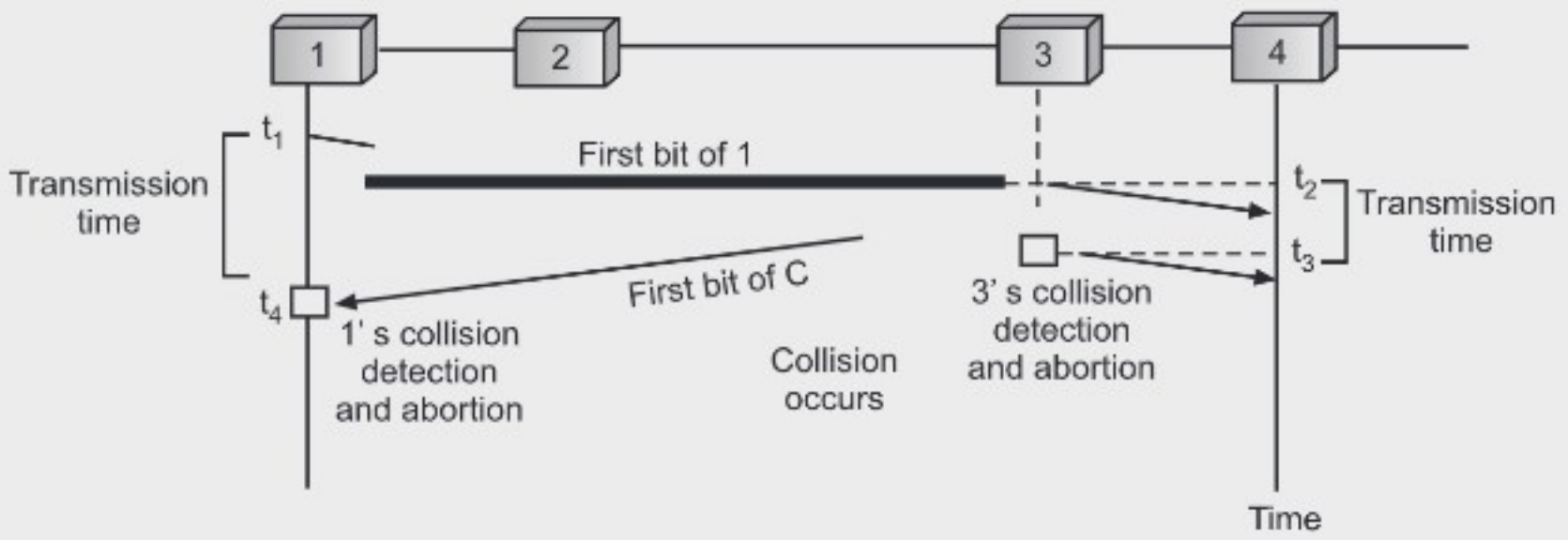


Fig. 4.43: Collision of the First Bit in CSMA/CD

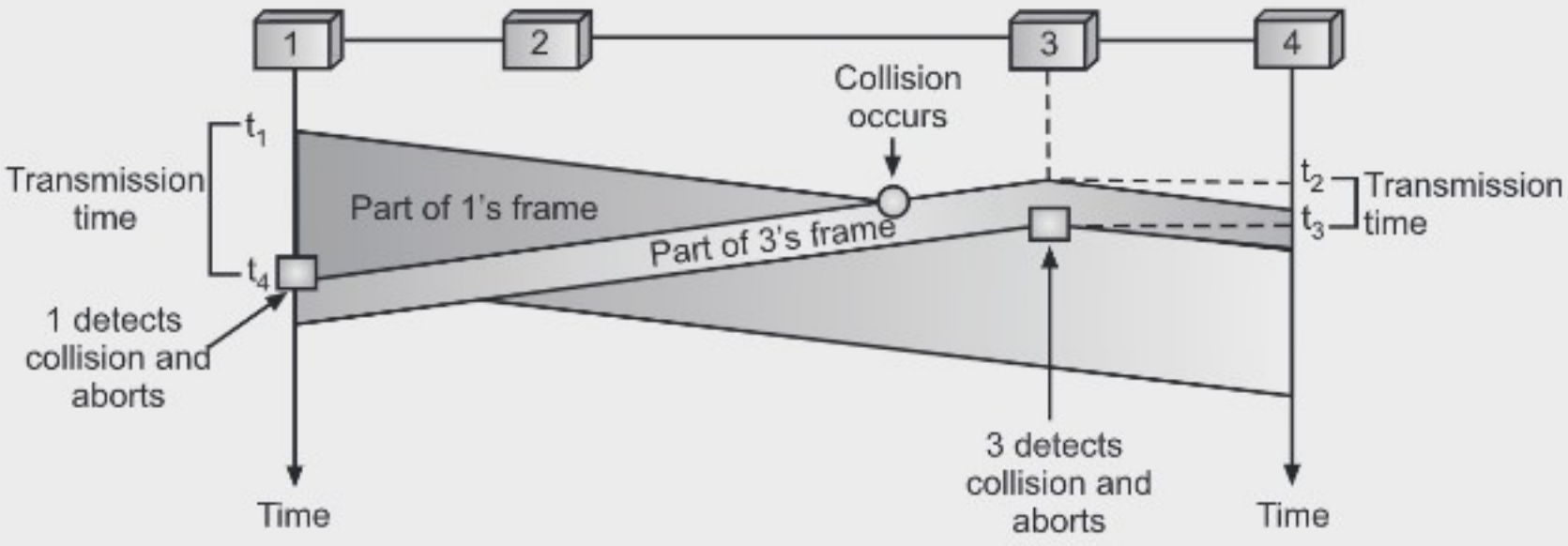


Fig. 4.44: Collision and Abortion in CSMA/CD

CSMA/CD Procedure:

- Fig. 4.45 shows a flow chart for the CSMA/CD protocol.

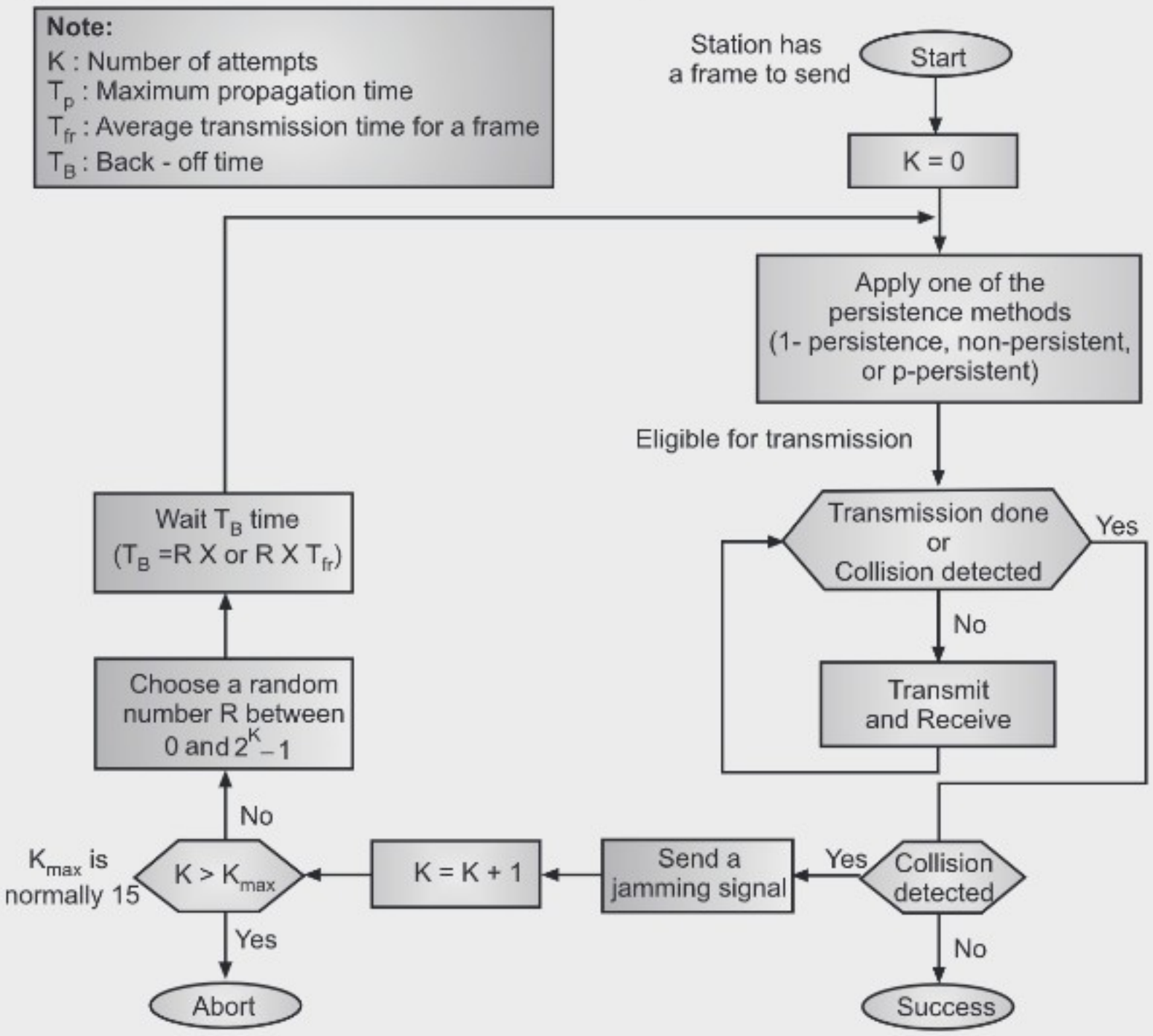


Fig. 4.45: Procedure for CSMA/CD

Explanation of Fig. 4.45:

- The station that has a ready frame sets the back off parameter to zero.
- Then it senses the line using one of the persistent strategies.
- It then sends the frame. If there is no collision for a period corresponding to one complete frame, then the transmission is successful.
- Otherwise the station sends the jam signal to inform the other stations about the collision.
- The station then increments the back off time and waits for a random back off time and sends the frame again.

- If the back off has reached its limit then the station aborts the transmission.
- CSMA/CD is used for the traditional Ethernet.
- CSMA/CD is an important protocol. IEEE 802.3 (Ethernet) is an example of CSMNCD. It is an international standard.
- The MAC sublayer protocol does not guarantee reliable delivery. Even in absence of collision the receiver may not have copied the frame correctly.

Advantages of CSMA/CD: **(S-19)**

1. Reliable because of collisions are detected and packets are re-sent, so no data is lost.
2. CSMA/CD has low overhead.
3. CSMA/CD is able to utilize all available bandwidth when possible.

Disadvantages of CSMA/CD:

1. Not useful for large/active networks.
2. In CSMA/CD collisions degrade network performance.
3. In CSMA/CD priorities cannot be assigned to certain nodes.
4. In CSMA/CD performance degrades exponentially as devices are added.

4.6.4 CSMA/CA

- CSMA/CA stands for Carrier Sense Multiple Access with Collision Avoidance.
- The basic idea behind CSMA/CD is that a station needs to be able to receive while transmitting to detect a collision.
- When there is no collision, station receives its own signal.
- When there is collision, the station receives two signals, its own and signals transmitted by another station. Station needs to distinguish between these two signals.
- In wired networks if collision occurs detected energy is almost double whereas in wireless networks much of the energy is lost in transmission only. So it becomes difficult to detect collision.
- There is need to avoid collision in wireless networks , because they cannot be detected. Carrier sense multiple access with collision avoidance (CSMA/CA) was invented for this network.
- CSMA/CA avoids the collisions using three basic techniques as shown in the Fig. 4.46..
  1. Inter frame space.
  2. Contention window.
  3. Acknowledgements.

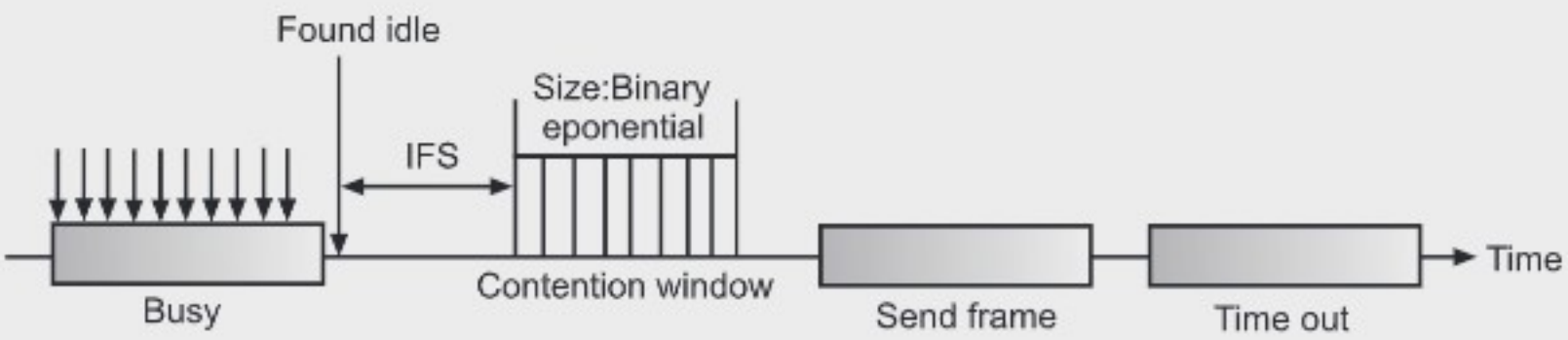


Fig. 4.46: CSMA/CA with Three States

1. **Inter-Frame Space (IFS):**

- Whenever the channel is found idle, the station does not transmit immediately. It waits for a period of time called Inter Frame Space (IFS).
- When channel is sensed to be idle, it may be possible that same distant station may have already started transmitting and the signal of that distant station has not yet reached other stations.
- Therefore, the purpose of IFS time is to allow this transmitted signal to reach other stations.
- If after this IFS time, the channel is still idle, the station can send, but it still needs to wait a time equal to contention time.
- IFS variable can also be used to define the priority of a station or a frame.

2. **Contention Window:**

- Contention window is an amount of time divided into slots.
- A station that is ready to send chooses a random number of slots as its wait time.
- The number of slots in the window changes according to the binary exponential back-off strategy. It means that it is set of one slot the first time and then doubles each time the station cannot detect an idle channel after the IFS time.
- This is very similar to the p-persistent method except that a random outcome defines the number of slots taken by the waiting station.
- In contention window the station needs to sense the channel after each time slot.
- If the station finds the channel busy, it does not restart the process. It just stops the timer and restarts it when the channel is sensed as idle.

3. **Acknowledgement:**

- Despite all the precautions, collisions may occur and destroy the data.
- The positive acknowledgment and the time-out timer can help guarantee that receiver has received the frame.

CSMA/CA Procedure:

- Fig. 4.47 shows the flow chart explaining the principle of CSMA/CA.

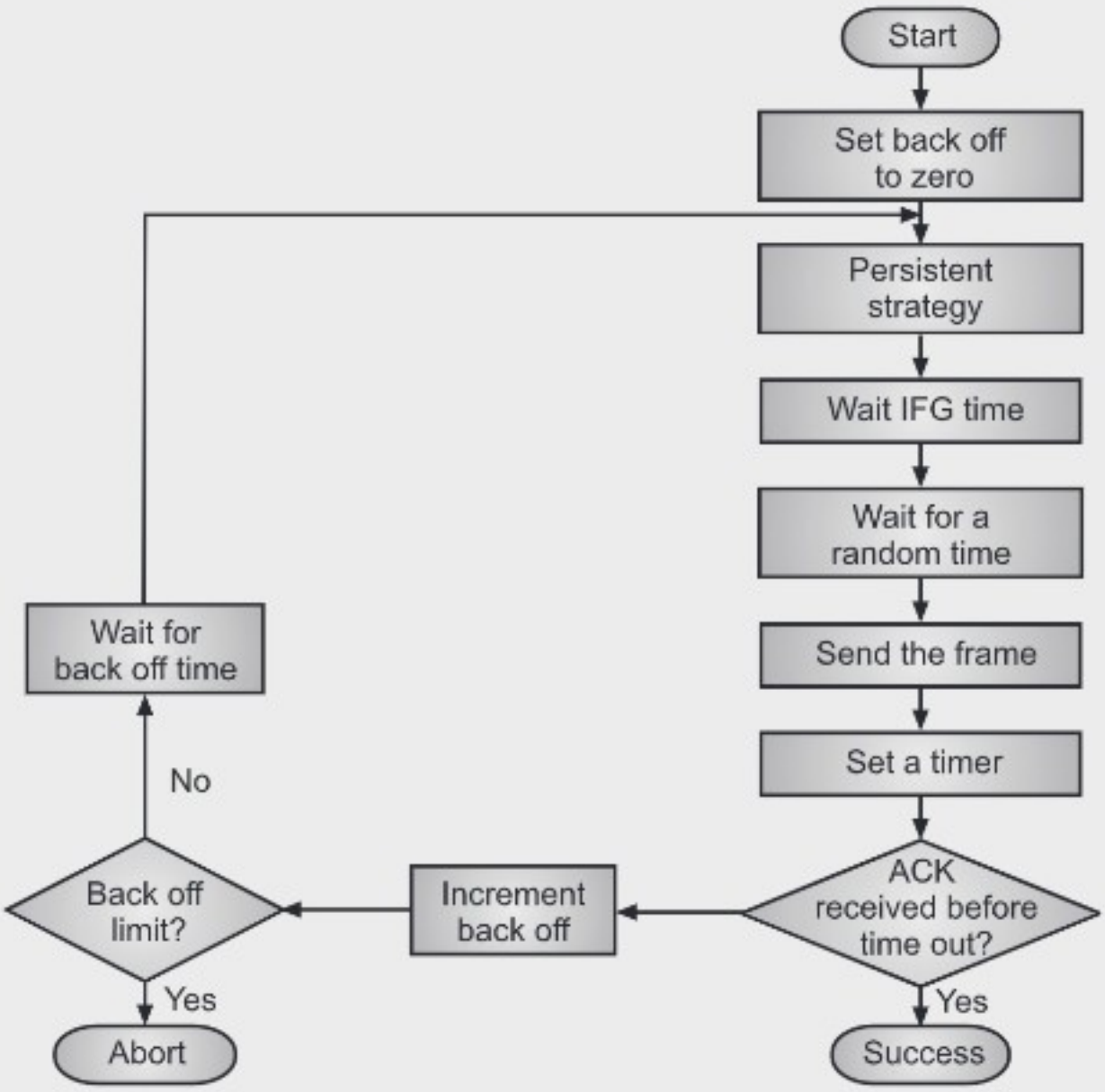


Fig. 4.47: Procedure of CSMA/CA

Explanation of Fig. 4.47:

- This is the CSMA protocol with collision avoidance.
- The station ready to transmit, senses the line by using one of the persistent strategies.
- As soon as it finds the line to be idle, the station waits for an IFG (Interframe gap) amount of time.
- If then waits for some random time and sends the frame.
- After sending the frame, it sets a timer and waits for the acknowledgement from the receiver.
- If the acknowledgement is received before expiry of the timer, then the transmission is successful.
- But if the transmitting station does not receive the expected acknowledgement before the timer expiry then it increments the back off parameter, waits for the back off time and resenses the line.

Advantages of CSMA/CA:

1. CSMA/CA is effective and it avoids data collisions.
2. CSMA/CA is reliable. Intent signals are sent until the cable is clear so that data will travel and reach its destination safely.

Disadvantages of CSMA/CA:

1. CSMA/CA is relatively slow. A signal of intent must be sent every time a computer wants to transmit causing signal traffic.
2. CSMA/CA is not useful for large/active networks.
3. CSMA/CA suffers from same distance limitations as CSMA/CD since it must listen for the signals of intent.

4.7 CONTROLLED ACCESS

- In controlled access, the stations consult each other to find which station has the right to send. A station cannot send unless it is authorized by other stations.
- Controlled access protocols grant permission to send data only to one node at a time, avoiding collision on the shared medium.
- There are three methods in the controlled access are:
  1. Reservation.
  2. Polling.
  3. Token passing.

4.7.1 Reservation

- In this method, the station needs to make a registration "before sending data".
- The time is divided into intervals. If there are m stations, then the intervals are exactly m.
- Each interval will belong to a station. In its own slot also, it has to make reservation to send the data frame.
- In each interval a reservation frame precedes the data frame.
- Fig. 4.48 shows this scenario.

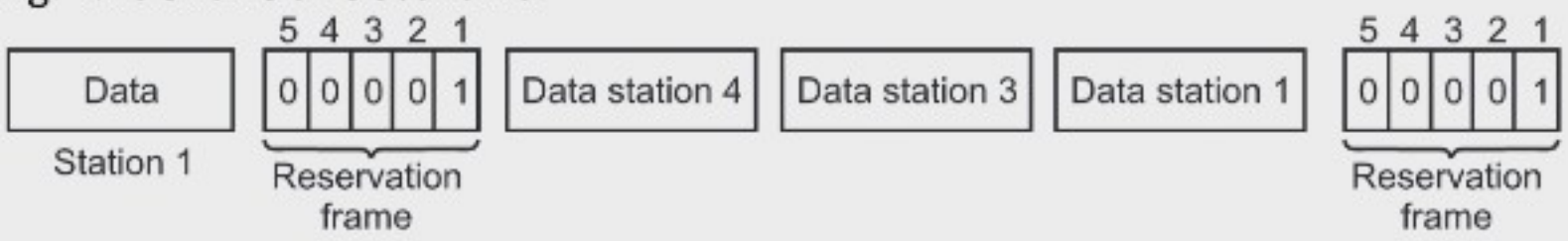


Fig. 4.48: Reservation Access Method

- Fig. 4.48 shows five stations. In the first, reservation frame stations 1, 3 and 4 have made the reservations.
- So the reservation frame is first followed by data frames of station 1, 3 and 4. In the second interval, only station 1 has made the reservation.

4.7.2 Polling (W-18)

- In this method, one station is designated as a primary station and others are secondary stations.
- All data exchanges must be made through the primary device even when the ultimate destination is a secondary device.

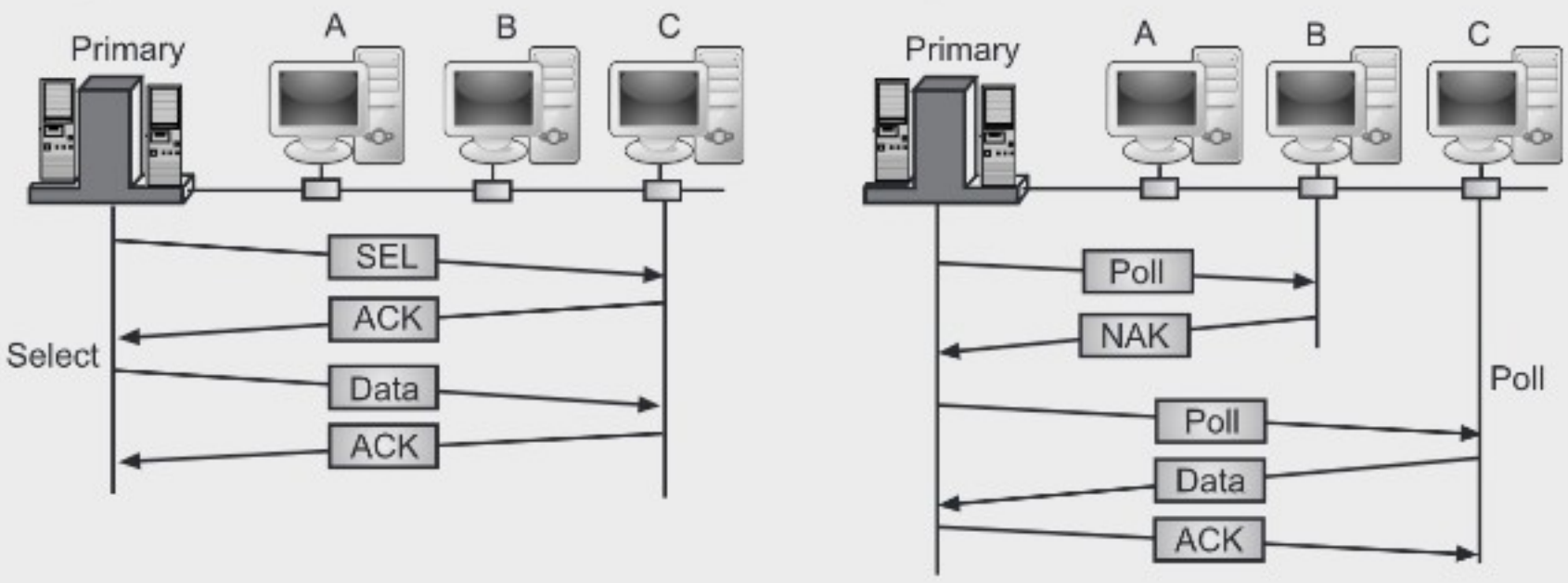
- The primary device controls the link; the secondary devices follow its instructions. It is up to the primary device to determine which device is allowed to use the channel at a given time. The primary device, therefore, is always the initiator of a session. If the primary station wants to receive data, it asks the secondary's if they have anything to send. This method is called as polling.
- If primary station wants to send data, it asks secondary station to receive the data. This is called as selecting.

1. **Select:**

- This is used when primary device sends the data.
- When primary station wants to send data to other machines, it should intimate the other secondary device that it is sending the data.
- To do this, the primary machine first sends the SEL frame in which the address of the machine (secondary machine) to which it wants to send the data is present.
- Then, the primary machine waits for the acknowledgement from that machine. Once the acknowledgement is reached then the data is send.

2. **Poll:**

- Whenever primary wants to receive data then polling is used. It polls each machine, if it has something to send.
- The secondary responds either with NAK frame which means nothing to send or with data frame if it wants to send data. If the response from the secondary device is negative i.e. received NAK frame then the next machine is polled until it finds one with data to send.
- When the primary machine gets the data, it accepts the data frame and returns the acknowledgement.
- Fig. 4.49 shows select and poll functions in polling access method.



(a) Select Function **(b) Poll Function**

Fig. 4.49 Select and Poll functions in polling access method

4.7.3 Token Passing (W-18)

- In this method, a station is allowed to send data when the station receives a special frame called token.
- In token passing, the stations are organized in the form of a logical ring. For every station there is predecessor and a successor.
- Control of the access to the medium is performed using a token. A token is a special bit pattern or a small packet, usually several bits in length, which circulate from node to node.
- The right to access the channel has been passed from predecessor to the current station. The right will be passed to the successor when the current station has no more data to send.
- The possession of the token gives the station the right to access the channel and send its data. Fig. 4.50 shows concepts of token passing.

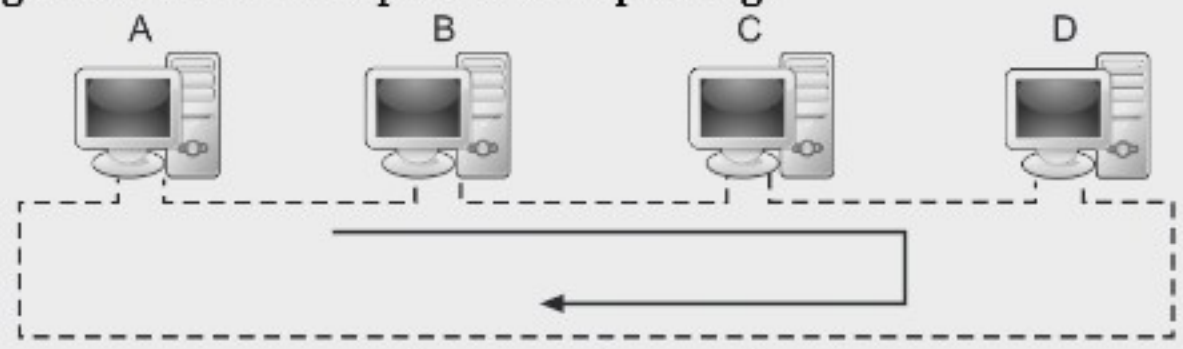


Fig. 4.50: Token Passing

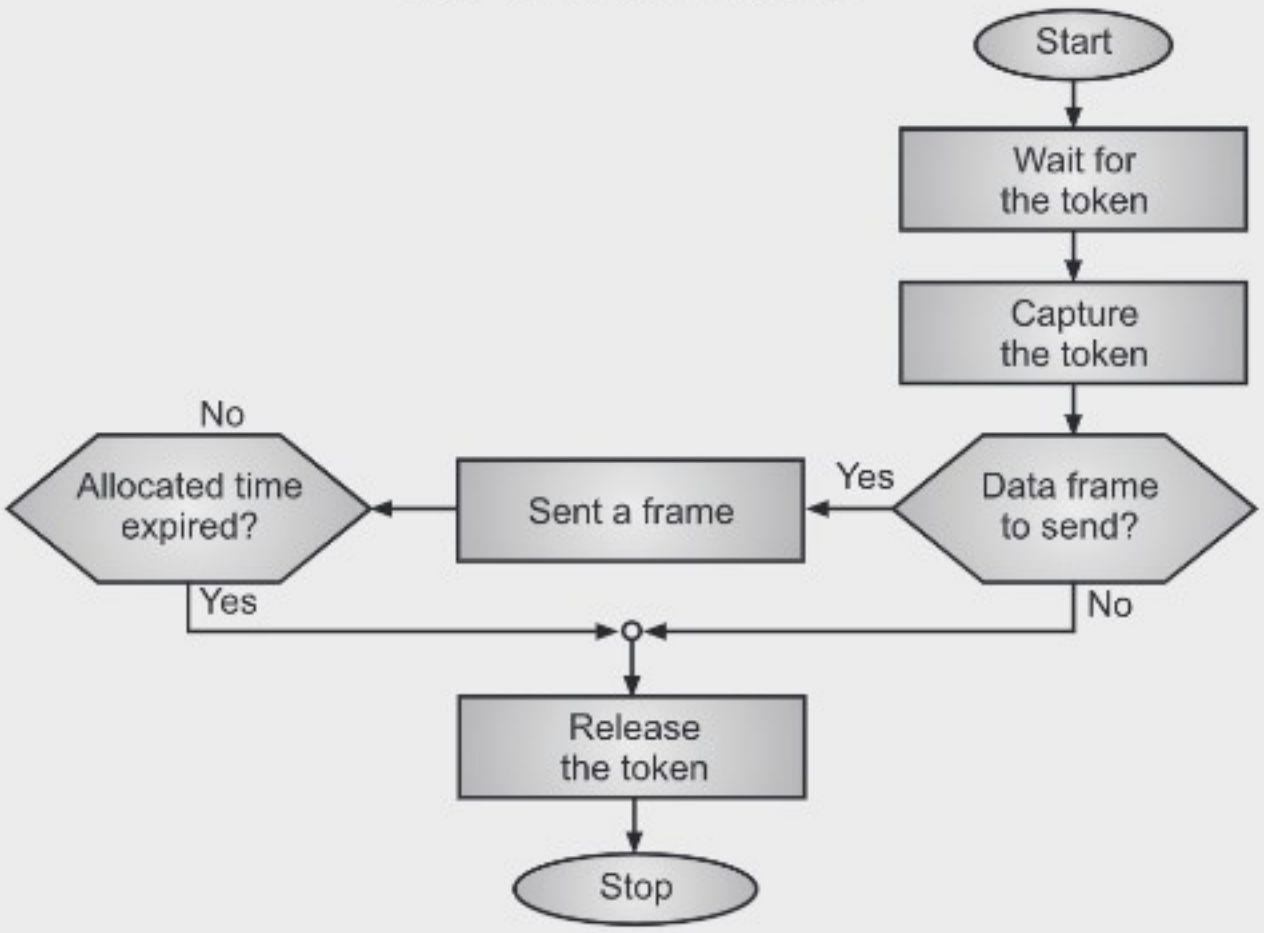


Fig. 4.51 Procedure of Token Passing

- When the channel is idle then the token circulates around the ring. When station wants to send data, it waits for a token, when the token comes, the station captures

the token and sends the data. When the machine finishes the data, it releases the token to the next machine (the successor).

- The station cannot send data until it receives the token again in the next round. In this process, when a station receives the token and has no data to send, it just passes the data to the next station.
- Token management is needed for this access method. Stations must be limited in the time they can have possession of the token. The token must be monitored to ensure it has not been lost or destroyed.
- The procedure is as shown in Fig. 4.51.

Advantages of Token Passing: **(S-18)**

1. In token passing no collisions mean more consistent performance in high-load configurations.
2. Token passing is effective because of collisions are prevented altogether.
3. Performance is consistently predictable, making token passing suitable for time sensitive applications.
4. Reliable because of the maximum amount of time before a given computer will be able to transmit can be calculated.
5. It is a non-contention method. Computers do not compete for access to the cable. Each computer will get its "turn" as the token comes around the network.

Disadvantages of Token Passing:

1. Slow because of a large amount of network bandwidth is consumed in the process.
2. The generation of a token creates network overhead.
3. In token passing the maximum speed is limited due to the overhead of token passing and re-generation.
4. Network hardware in token passing is more complex and expensive than that used with other access methods.

4.8 CHANNELIZATION (W-18; S-18)

- Channelization is the multiple access method in which the available bandwidth of a link is shared in time, frequency or through code between different stations.
- Three channelization protocols are present in networking as shown in Fig. 4.52.
- Sometimes, channelization also called as channel partition.
- Fig. 4.52 shows following channelization protocols.

1. **FDMA (Frequency Division Multiple Access):** Here, the bandwidth is shared by all stations. Each band is given to the station. Station sends data in its allocated band. The band belongs to the station all the time. It is data link layer protocol. Here, the bandwidth is divided into channels.

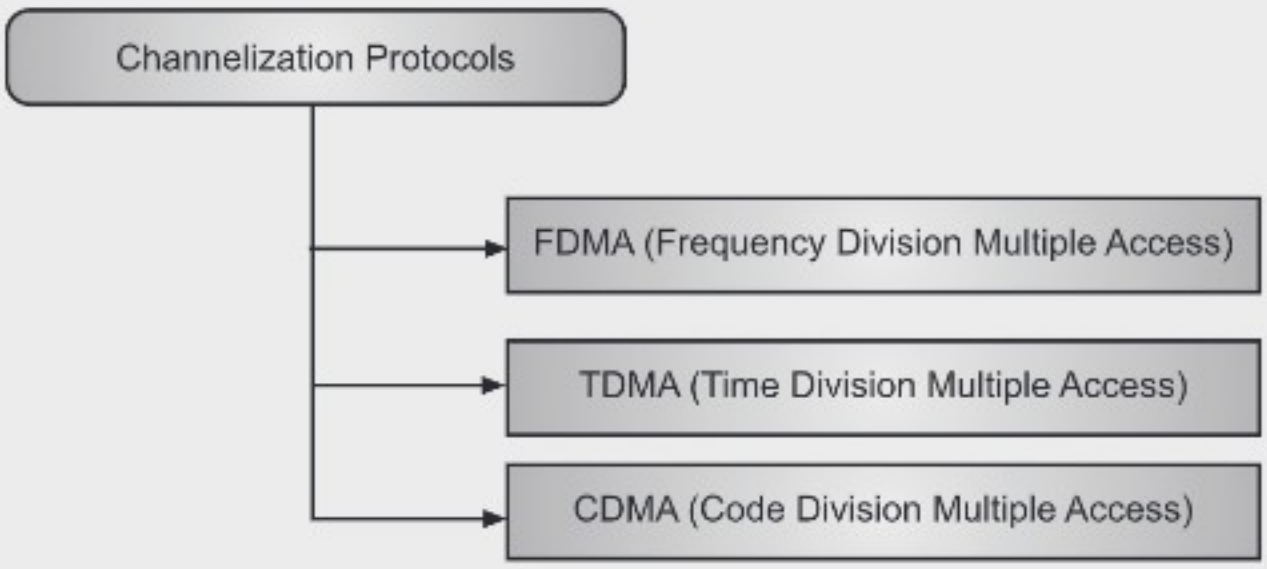


Fig. 4.52: Channelization Protocols

2. **TDMA (Time Division Multiple Access):** The entire bandwidth is one channel. Each station is allocated a time slice. During its time slice, the data is send.
3. **CDMA (Code Division Multiple Access):** Here, only one channel occupies the entire bandwidth of the link. All stations can send data simultaneously. Here, the channel carries all transmissions simultaneously. Each station is assigned a code which is a sequence number called chip.

4.8.1 FDMA

- FDMA is a channel access method used in multiple-access protocols as channelization protocol.
- In FDMA, the available bandwidth is divided into various frequency bands.
- Each station is allocated a band to send its data. This band is reserved for that station for all the time.
- Each station also uses a band pass filter to confine the transmitter frequencies.
- The frequency bands of different stations are separated by small bands of unused frequency. These unused frequency bands are called guard bands that prevent station interferences.
- FDM is a physical layer technique whereas FDMA is an access method in the data link layer. The data link layer in each station tells its physical layer to make a band pass signal from the data passed to it. The signal must be created in the allocated band.
- So FDMA is the process of dividing one channel or bandwidth into multiple individual bands, each for use by a single user. Each individual band or channel is wide enough to accommodate the signal spectra of the transmissions to be propagated. The data to be transmitted is modulated on to each subcarrier, and all of them are linearly mixed together.
- The best example of FDMA is the cable television system.
- Fig. 4.53 shows FDMA concept.

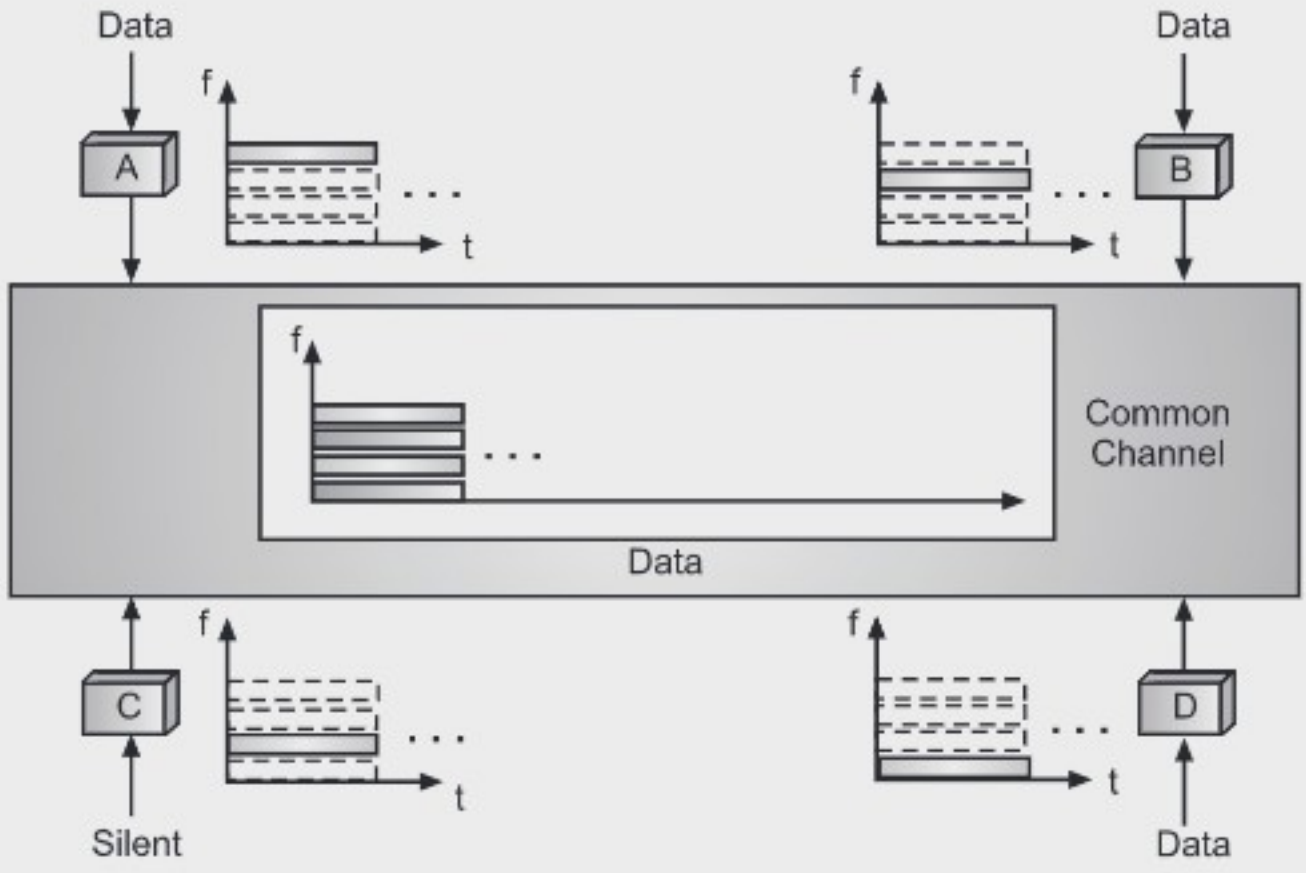


Fig. 4.53: FDMA

Advantages of FDMA:

1. A continuous transmission scheme and therefore of lower complexity.
2. FDMA technology is mature and cost is low.
3. Simple to implement from a hardware stand-point, because multiple users are isolated by employing simple band pass filters.
4. No channel equalization required in FDMA.

Disadvantages of FDMA:

1. Channel allocation is not flexible in FDMA.
2. In FDMA network and spectrum planning are intensive.
3. In FDMA frequency planning is time consuming.
4. FDMA requires unlink power control to maintain link quality.

4.8.2 TDMA

- TDMA is a channel access method for stored medium networks.
- In time-division multiple access (TDMA) stations share the bandwidth of the channel in time. Every station is allocated a time slot, in which it can send data.
- In TDMA, the bandwidth is just one channel that is timeshared between different stations.
- The main problem with TDMA lies in achieving synchronization between the different stations. Each station needs to know the beginning of its slot and the location of its slot. This may be difficult because of propagation delays introduced in the system if the stations are spread over a large area.

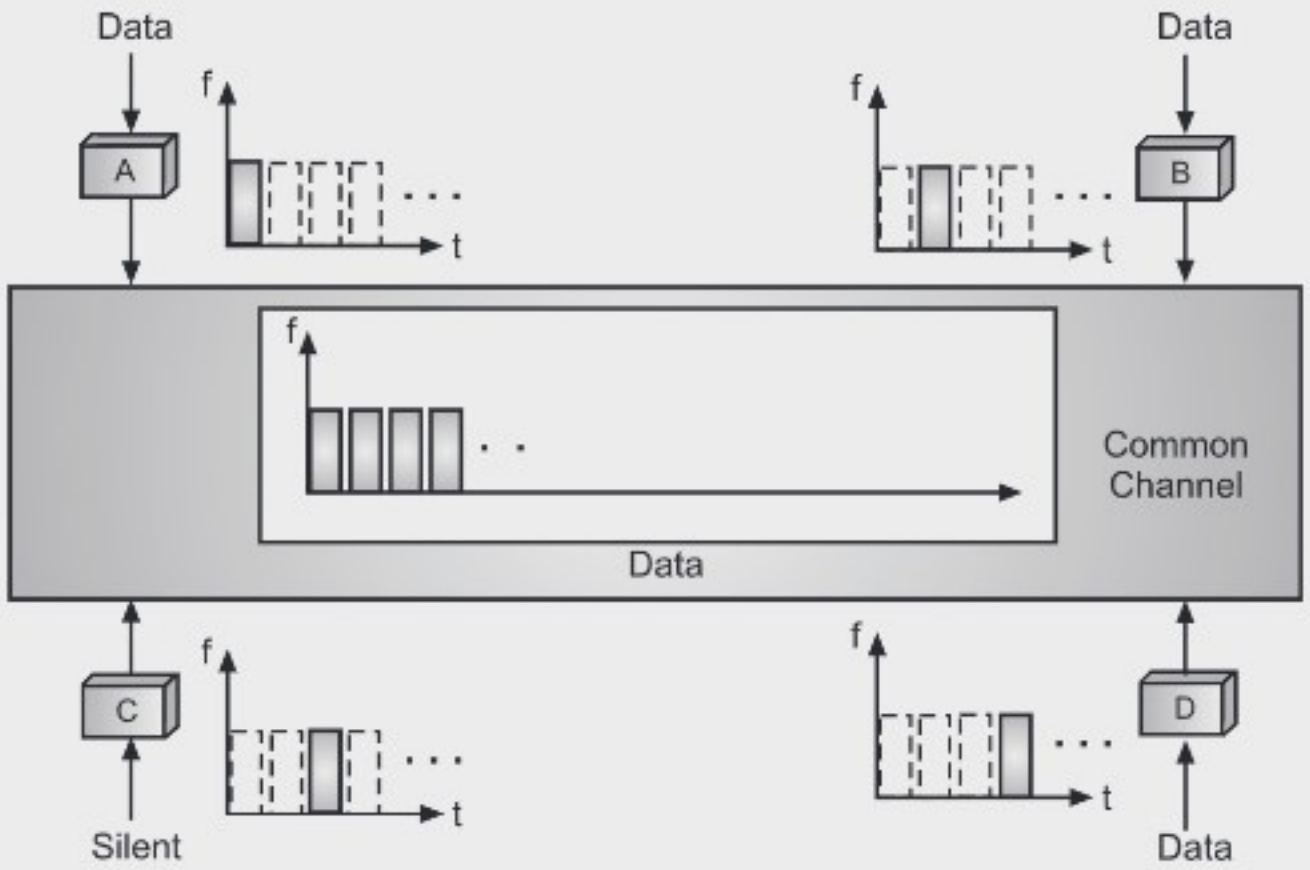


Fig. 4.54: TDMA

- TDMA and TDM are seems to be conceptually same, but they are different. TDM is a physical layer technique that combines the data from slower channels and transmits them by using a faster channel. The process uses a physical multiplexer that interleaves data units from each channel, whereas TDMA is Data link layer access method. The Data link layer in each station tells its Physical layer to use the allocated time slot.
- TDMA is used in digital mobile radio systems.

Advantages of TDMA:

1. TDMA is most efficient method of transmission because of efficient use of transmission resources.
2. At a given time only one carrier is present on the channel hence intermodulation distortion is eliminated.
3. TDMA is more flexible than FDMA because of TDMA can accommodate a wider range of bit rates by allowing a station to be allocated several slots.
4. TDMA transmission is separated in time domain. Processing of signal in time domain is easier and simpler.

Disadvantages of TDMA:

1. Bit and frame timings must be maintained by TDMA.
2. Precise synchronization between stations is required. Transmission of every station must occur during exact time slot.

4.8.3 CDMA

- CDMA (Code Division Multiple Access) also called spread-spectrum and code division multiplexing, one of the competing transmission technologies for digital mobile phones.

- In CDMA, Data from all stations are transmitted simultaneously and are separated based on coding theory.
- In TDMA and FDMA the transmissions from different stations are clearly separated in either time or frequency.
- In case of CDMA, the transmissions from different stations occupy the entire frequency band at the same time.
- Multiple simultaneous transmissions are separated by using coding theory.
- Each bit is assigned a unique m-bit code or chip sequence.

Advantages of CDMA:

1. High immunity for interference and jamming.
2. CDMA does not require any time synchronization among the stations.
3. In CDMA each stations can use entire bandwidth at any time.
4. CDMA offers highly secured communication.

Disadvantages of CDMA:

1. Low throughput efficiency.
2. The overall performance degrades with increase in number of users.

Summary

- The Data Link Layer is the second layer in the OSI model. The main functions of the data link layer are providing the service interface to the network layer and Dealing with the transmission errors.
- The data link layer services differ from system to system. The three main services are unacknowledged connectionless service, acknowledged connectionless service and acknowledged connection oriented service.
- In unacknowledged connectionless service the source machine send independent frames to the destination machine without having the destination machine acknowledge them.
- When acknowledged connectionless service is offered, there are still no logical connections used, but each frame sent is individually acknowledged.
- With acknowledged connection oriented service, the source and destination machines establish a connection before any data are transferred.
- The data link layer on the receiving end remove the escape byte before the data are given to the network layer. This is known as byte stuffing or character stuffing.
- The most popular error detection technique is based on polynomial is called as CRC (cyclic redundancy check).
- The device that can be used to interconnect two separate LANs is known as a bridge.
- ALOHA is a system for coordinating and arbitrating access to a shared communication Networks channel.
- The original ALOHA protocol is called pure ALOHA.
- Slotted ALOHA was invented to improve the efficiency of pure ALOHA as chances of collision in pure ALOHA are very high.

- In slotted ALOHA, the time of the shared channel is divided into discrete intervals called slots.
- CSMA is a network access method used on shared network topologies such as Ethernet to control access to the network.
- In 1-persistent CSMA method, station that wants to transmit data continuously senses the channel to check whether the channel is idle or busy. If the channel is busy, the station waits until it becomes idle.
- P-persistent CSMA method is used when channel has time slots such that the time slot duration is equal to or greater than the maximum propagation delay time.
- In non-persistent CSMA, a station that has a frame to send senses the channel. If the channel is idle, it sends immediately. If the channel is busy, it waits for a random amount of time and then senses the channel again.
- CSMA/CD (Carrier Sense Multiple Access with Collision Detection) protocol can be considered as a refinement over the CSMA.
- The basic idea behind CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) is that a station needs to be able to receive while transmitting to detect a collision.
- Whenever the channel is found idle, the station does not transmit immediately. It waits for a period of time called Inter Frame Space (IFS).
- In Reservation method, the station needs to make a registration "before sending data".
- In Polling method, one station is designated as a primary station and others are secondary stations.
- In Token Passing method, a station is allowed to send data when the station receives a special frame called token.
- In token passing, the stations are organized in the form of a logical ring. For every station there is predecessor and a successor.
- Channelization is the multiple access method in which the available bandwidth of a link is shared in time, frequency or through code between different stations.
- Channelization protocols are FDMA (Frequency Division Multiple Access) here, the bandwidth is shared by all stations, TDMA (Time Division Multiple Access) here, the entire bandwidth is one channel. Each station is allocated a time slice. During its time slice, the data is send and CDMA (Code Division Multiple Access) here, only one channel occupies the entire bandwidth of the link. All stations can send data simultaneously.

Check Your Understanding

1. Which error detection method involves polynomials?
   (a) Simple parity check (b) 2-D parity check
   (c) CRC (d) Checksum.

2. In cyclic redundancy checking what is the CRC?
   (a) The divisor (b) The quotient
   (c) The dividend (d) The remainder.
3. In cyclic redundancy checking the divisor is _____ the CRC.
   (a) The same size as (b) 1 bit less than
   (c) 1 bit more than (d) 2 bit more than.
4. Which one of the following is the multiple access protocol for channel access control?
   (a) CSMA/CD (b) CSMA/CA
   (c) Both (a) and (b) (d) None of the mentioned.
5. In _____ each station sends a frame whenever it has a frame to send.
   (a) Pure ALOHA (b) Slotted ALOHA
   (c) both (a) and (b) (d) Neither (a) nor (b).
6. In the _____ method, after the station finds the line idle, it sends its frame immediately. If the line is not idle, it continuously senses the line until it finds it idle.
   (a) Nonpersistent (b) 1-persistent
   (c) P-persistent (d) None of the above.
7. In _____ methods, the stations consult one another to find which station has the right to send.
   (a) Random access (b) Controlled access
   (c) Channelization (d) None of the above.
8. In the _____ method, each station has a predecessor and a successor.
   (a) Reservation (b) Polling
   (c) Token passing (d) None of the above.
9. In _____, the available bandwidth is divided into frequency bands.
   (a) FDMA (b) TDMA
   (c) CDMA (d) None of the above.
10. In _____, the sequences are generated using orthogonal codes such the Walsh tables.
   (a) FDMA (b) TDMA
   (c) CDMA (d) None of the above.

ANSWER KEY

1. (c)	2. (d)	3. (c)	4. (c)	5. (a)
6. (b)	7. (b)	8. (c)	9. (a)	10. (c)

Practice Questions

Q.1: Answers the Following Questions in short.

1. What is channelization?
2. What are different framing methods?
3. What is meant by byte stuffing?
4. What is meant by CRC?

5. Which are the type of errors?
6. List out the random access protocols.
7. List out persistence methods.

Q.2: Answers the Following Questions.

1. Explain the concept of framing in detail in data link layer
2. Explain error detection at the data link layer.
3. The 10 bit sequence is 1010011110 and the divisor of 1011. Find the CRC.
4. Explain the pure aloha and slotted aloha.
5. Compare and contrast between controlled accesses over random access.
6. What is the difference between polling and selecting?
7. What is chip sequence?
8. Write short note on:
   (i) 1-persistent CSMA,
   (ii) Non-persistent CSMA.
9. Write short notes on:
   (i) ALOHA (ii) CSMA (iii) CSMA / CD
   (iv) CSMA/CA (v) Walsh table.
10. Explain the following terms:
    (i) TDMA (ii) FDMA (iii) CDMA.

Q.3: Define the terms.

1. Framing
2. Channelization
3. Random access protocols
4. Pure ALOHA
5. Slotted ALOHA

Previous Exams Questions

Summer 2019

1. In token passing method, each station has a predecessor and ..... **[1 M]**
(i) End **(ii) Successor**
(iii) First (iv) None of the above

2. What are the types of Errors ? **[1 M]**

Ans. Refer to section 4.3

3. Write a note on framing methods in data link layer. **[4 M]**

Ans. Refer to section 4.2.2

4. Explain slotted ALOHA in detail. **[4 M]**

Ans. Refer to section 4.6.1.2

5. State advantage of CSMA/CD. **[3 M]**

Ans. Refer to section 4.6.3

6. Explain error detection code CRC. [3]

Ans. Refer to section 4.3.2

Winter 2018

1. In.....available bandwidth is divided into frequency bands. **[1 M]**

(i) FDMA (ii) TDMA

(iii) CDMA (iv) CSMA/CA

2. Define channelization. **[1 M]**

Ans. Refer to section 4.8.

3. Define PURE ALOHA. Explain frames in it with diagram. **[4 M]**

Ans. Refer to section 4.6.1.1

4. Explain Token passing in detail. **[5 M]**

Ans. Refer to section 4.7.3

5. What is difference between polling and selecting ? **[4 M]**

Ans. Refer to section 4.7.2

6. Write a short note on CSMA/CD. **[4 M]**

Ans. Refer to section 4.6.3

Summer 2018

1. Which one of the following is the multiple access protocol for channel access control? **[1 M]**

(a) CSMA/CD (b) CSMA/CA

(c) Both (a) and (b) (d) None of the mentioned.

2. In _____, the available bandwidth is divided into frequency bands. **[1 M]**

(a) FDMA (b) TDMA

(c) CDMA (d) None of the above.

3. Define channelization. **[1 M]**

Ans. Refer to section 4.8

4. List the framing methods in Data link layer. **[1 M]**

Ans. Refer to section 4.2.2

5. Give the advantages of token passing. **[4 M]**

Ans. Refer to section 4.7.3

6. Write short note on Cyclic Redundancy Check. **[5 M]**

Ans. Refer to section 4.3.2

7. State the advantages and disadvantages of Non persistant CSMA. **[3 M]**

Ans. Refer to section 4.6.2.2

8. Given the dataword 1010011110 and the divisor 10111 **[4 M]**

(a) Show the generation of the codeword at the sender site (using binary division).

(b) Show the checking of the codeword at the receiver site (assume no error).

Ans. Refer to Example 1

❖❖❖

5...

Network Layer

Objectives...

- To understand Concepts of Network Layer and its Functions
- To study Logical Addressing
- To learn IPv4 Protocol and IPv6 Protocol

5.1 INTRODUCTION

- In the seven layer OSI model of computer networking, the network layer is layer 3. Network layer receives services from the data link layer and gives services to the transport layer. Fig. 5.1 shows the function of network layer.

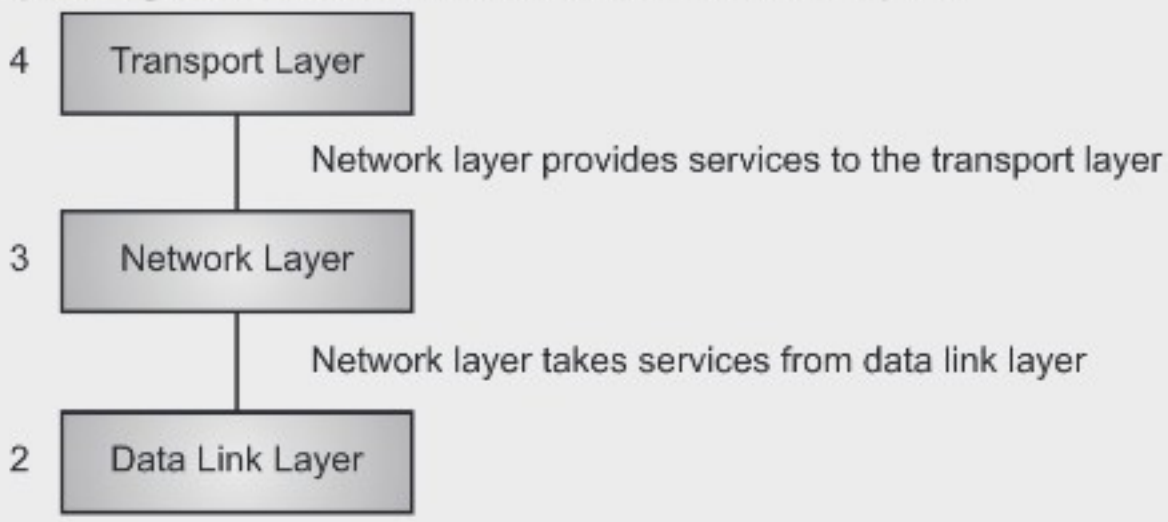


Fig. 5.1: Function of Network Layer

- The network layer is responsible for the delivery of individual packets from the source to the destination host.
- Network layer is also responsible for routing mechanism, addressing, internet-working, packetizing and fragmentation etc.

Functions Performed by Network Layer: **(W-18)**

1. **Internetworking:** One of the main responsibilities of a network layer is to provide internetworking between different networks. It provides a logical connection between different types of network. Because of this layer, we can combine various different networks to form a bigger network.

2. **Logical Addressing:** Large numbers of different networks can be combined together to form bigger networks or internetwork. In order to identify each device on internetwork uniquely, the network layer defines an addressing scheme. Such an address distinguishes each device uniquely and universally.
3. **Routing:** When independent networks or links are combined together to create internet works, multiple routes are possible from source machine to destination machine. The network layer protocols determine which route or path is best from source to destination. This function of the network layer is known as routing. Network layer routes frames among networks.
4. **Packetizing:** The network layer receives the data from the upper layers and creates its own packets by encapsulating these packets. The process is known as packetizing. This packetizing is done by Internet Protocol (IP) that defines its own packet format. The network layer encapsulates packets received from upper layer protocols and makes new packets out of them.
5. **Fragmentation:** Fragmentation means dividing the larger packets into small fragments. The maximum size for a transportable packet is defined by physical layer protocol. For this, the network layer divides the large packets into fragments so that they can be easily sent on the physical medium. If it determines that a downstream router's Maximum Transmission Unit (MTU) size is less than the frame size, a router can fragment a frame for transmission and re-assembly at the destination station.

5.2 IPV4 ADDRESSES

- A computer somewhere in the world needs to communicate with another computer, (using the Internet).
- The packets transmitted by the source computer may pass through several LANs or WANs before reaching at the destination computer.
- For such communication, to identify every device uniquely on Internet, we need a global addressing scheme, called logical addressing.
- A logical address is given to all hosts connected to the Internet and this logical address is called Internet Protocol Address or IP address.
- Today, we use the term IP address (Internet Protocol address) to mean a logical address in the network layer of the TCP/IP protocol suite. By using an IP address, we can identify a computer or device on a TCP/IP network.

Concept of IP Address:

- An IP address or logical address is an identifier assigned to each computer and other device (e.g., printer, router etc.) connected to a TCP/IP network that is used to locate and identify the node in communications with other nodes on the network.
- Fig. 5.2 shows an IP address format. An IP address consists of two parts i.e., the network ID and the host ID.

- The **network ID** is used to identify a specific network or subnet, whereas the **host ID** identifies the hosts on a given network or subnet. For example, with the IP address of 132.10.26.2 and the default subnet mask of 255.255.0.0, the network ID is 132.10 and the host ID is 26.2.
- The 32-bit IP address is grouped eight bits segments (octets) at a time, separated by dots and represented in decimal format known as dotted decimal notation.
- Each bit in the octet has a binary weight (128, 64, 32, 16, 8, 4, 2, 1). The minimum value for an octet is 0, and the maximum value for an octet is 255.

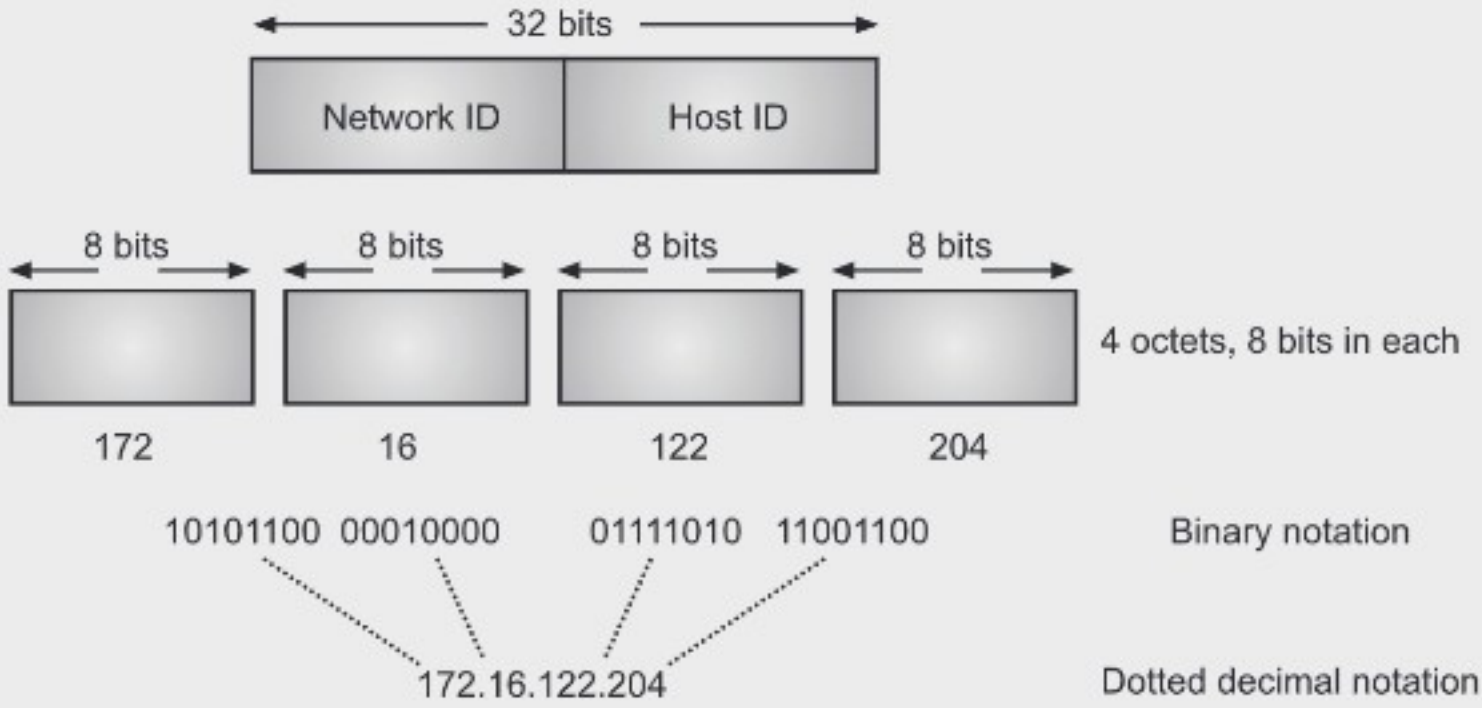


Fig. 5.2: Format of an IP Address

- There are two types of IP addresses IPv4 and IPv6.
- Version 4 of the Internet Protocol (IPv4) defines an IP address as a 32-bit number. However, because of the growth of the Internet and the depletion of available IPv4 addresses, a new version 6 of IP (IPv6), using 128 bits for the IP address was developed in 1995.
- IPv4 addresses are 32 bits in length and the IPv6 addresses use 128-bit addresses, which give much greater flexibility in address allocation.
- Internet Protocol version 4 (IPv4) is the fourth version in the development of the Internet Protocol (IP).
- IPv4 is one of the core protocols of standards-based internetworking methods in the Internet.
- An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a device such as a computer or a router to the Internet.
- IP addresses are unique. Each address defines one, and only one, connection to the Internet.
- Two devices on the Internet can never have the same address at the same time. An address is assigned to a device for a time period, generally by ISP (Internet service provider) and then taken away and assigned to another device.
- The IPv4 addresses are universal in the sense that the addressing system must be accepted by any host that wants to be connected to the Internet.

5.2.1 Address Space, Notations

Address Space:

- IPv4 protocol defines addresses that have an address space. An address space is the total number of addresses used by the protocol.
- IPv4 uses 32-bit addresses, which means the address space is 2^{32} or 4,294,967, 296 (more than 4 billion), this means if there were no restrictions, more than 4 billion devices could be connected to the Internet.

Notations:

IPv4 addresses are defined by two different types of notations i.e., Binary notation and Dotted decimal notation.

1. **Binary Notation:**

- In the binary notation method, to represent binary address, '0' and '1' are used.
- Length of address is 32 bits, which is grouped into 4 octet. Each octet is referred to as a byte. But such addresses are difficult to remember.

  For example, 01010111 10010101 00011101 00000011

2. **Dotted Decimal Notation:**

- Representing a IPv4 address by using binary notation is very long and not easier to read.
- To make the IPv4 address more compact and easier to read, Internet addresses are usually written in dotted decimal form. Dots are used to separate the bytes.

  For example, 117.146.15.10.
- Fig. 5.3 shows IPv4 address in both binary and dotted decimal notation. Each byte (octet) is 8 bits, each number in dotted-decimal notation is a value ranging from 0 to 255.

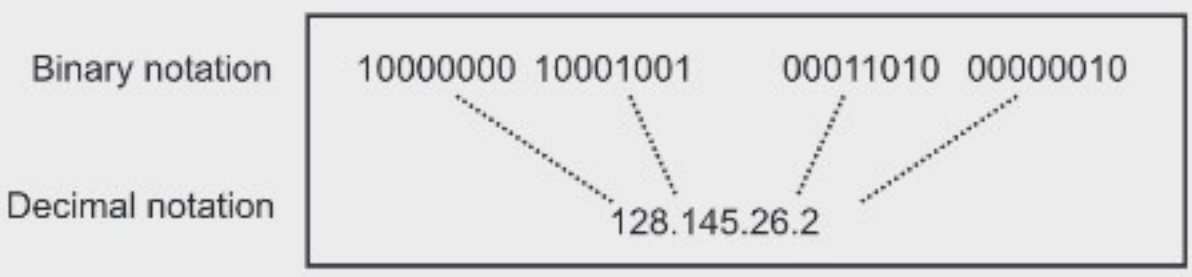


Fig. 5.3: Dotted Decimal Notation and Binary Notation for IPv4

Examples 1: Convert the following IPv4 addresses from binary notation to decimal notation.

(i) 01110101 10010101 00011101 00000100, and

(ii) 10000001 00001011 00001001 11101111.

Solution: (i) 117.149.29.4

(ii) 129.11.9.239.

Examples 2: Convert the following IPv4 addresses from decimal notation to binary Notation if it is in correct form. **(S-18)**

(i) 128.29.4.31

(ii) 221.34.7.82

(iii) 221.36.3.4.5

(iv) 129.300.4.10.

Solution: (i)10000000 00011101 00000100 00011111.

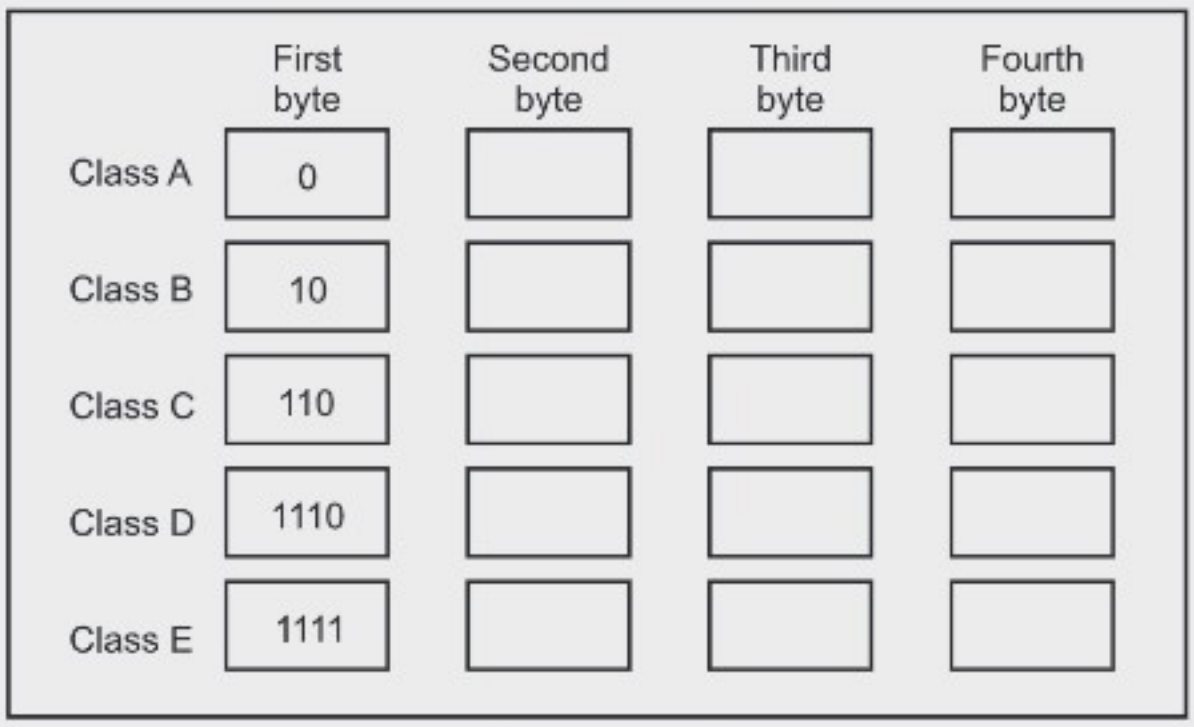
(ii) 11011101 00100010 00000111 01010010.

(iii)There is an error, no more than 4 numbers in an IPv4 address.

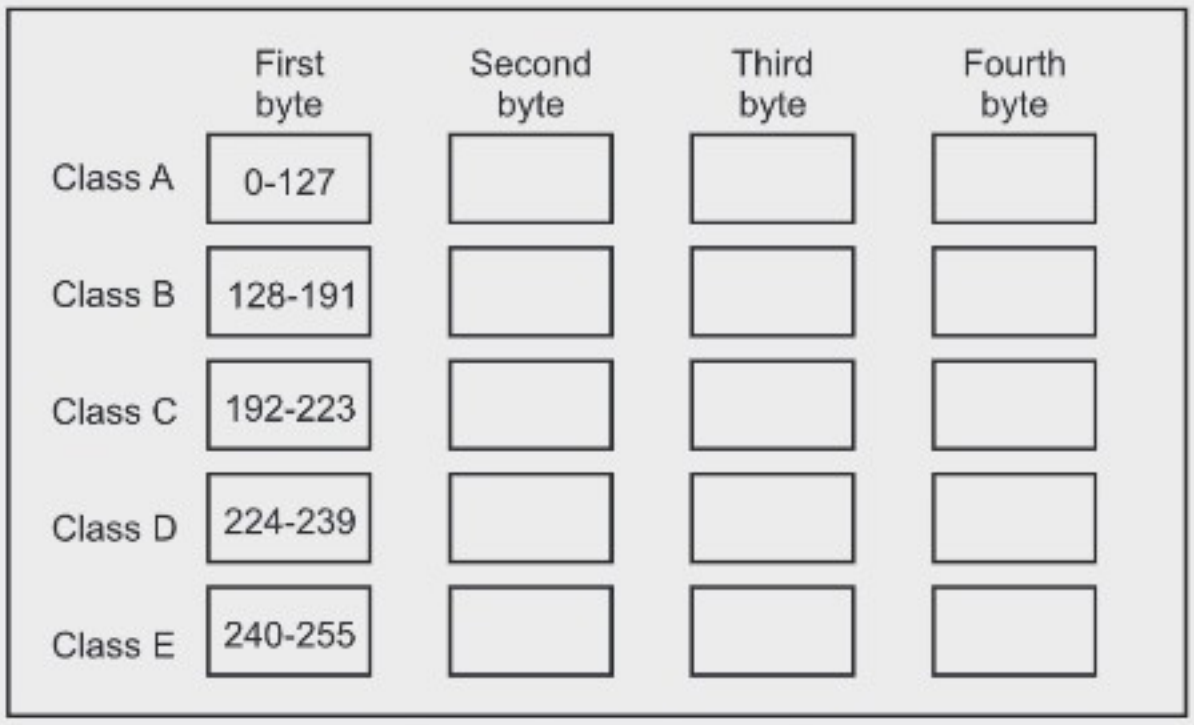
(iv)There is an error, Each number should be less than or equal to 255 (300 is out of range).

5.2.2 Classful Addressing

- IPv4 addressing uses the concept of classes. This architecture is called classful addressing.
- Although the classful addressing scheme is becoming obsolete, it is worth to understanding it.
- In classful addressing, the address space is divided into five classes: A, B, C, D and E. Each class occupies some part of the address space.
- We can find the class of address just by checking the first few bits, if address is binary notation and checking the first byte if address is dotted decimal. Fig. 5.4 shows both methods.



(a) Binary Notation



(b) Dotted Decimal Notation

Fig. 5.4: Finding the Classes in Binary and Dotted Decimal Notations

Classes and Blocks:

- One problem with classful addressing is that each class is divided into a fixed number of blocks with each block having a fixed size as shown in Table 5.1.

Table 5.1: Number of blocks size in classful IPv4 addressing

Class	Number of blocks	Block size	Application
A	128	16, 777, 216	Unicast
B	16, 387	65, 536	Unicast
C	2, 097, 152	256	Unicast
D	1	268, 435, 456	Multicast
E	1	268, 435, 456	Reserved

- Class A addresses were designed for large organizations with a large number of attached hosts or routers.
- Class B addresses were designed for mid-size organizations with tens of thousands of attached hosts or routers.
- Class C addresses were designed for small organizations with a small number of attached hosts or routers.
- Class D addresses were designed for multicasting and class E addresses were reserved for future use.

Netid and Hostid: **(W-18, S-18)**

- In classful addressing, an IP address in class A, B or C is divided into Netid and Hostid. Netid and Hostid are varying in lengths depending on class of the address. Fig. 5.5 shows Netid and Hostid.

- In class A, one byte defines Netid and three bytes defines the Hostid. In class B, two bytes defines the Netid and two bytes defines the Hostid. In class C, three bytes defines the Netid and one byte defines the Hostid.

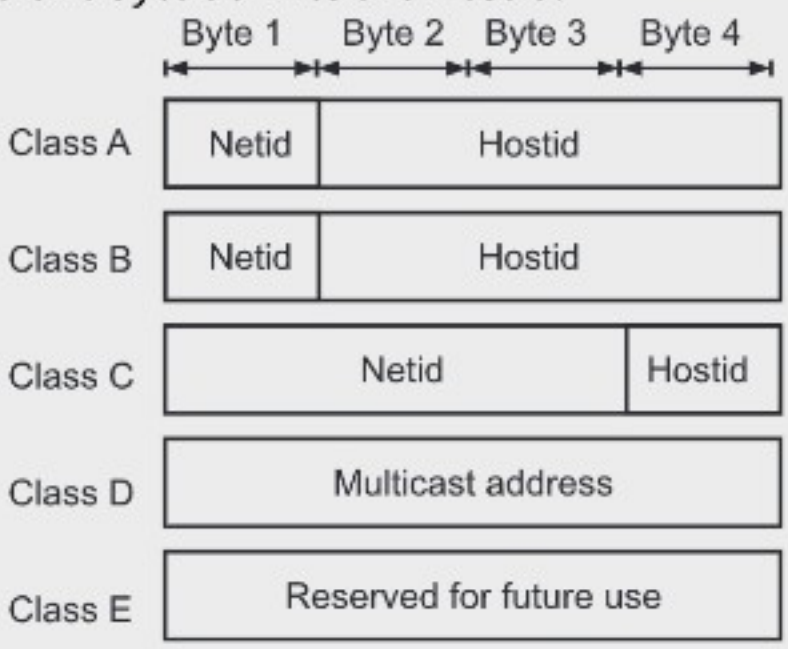


Fig. 5.5: Netid and Hostid

For example:

1. 00000001 00001011 00001011 11101111

   The first bit of this address is 0. This is a class A address. Since it is class A address Netid is 00000001 and Hostid is 00001011 00001011 11101111

2. 130. 45. 23. 120

   The first byte of this address is in between 128 to 191, so this address is class B. Its Netid is 130. 45. 0. 0 and Hostid is 23. 120

Mask:

- Netid and Hostid is predetermined in classful addressing. We can also use a mask (default mask), a 32 bit number made up of contiguous 1s is followed by contiguous 0s to find Netid and Hostid.
- The masks for classes A, B and C are shown in Table 5.2.

Table 5.2: Default mask for classful addressing

Class	Binary	Dotted decimal	CIDR
A	11111111 00000000 00000000 00000000	255. 0. 0. 0	/8
B	11111111 11111111 00000000 00000000	255. 255. 0. 0	/16
C	11111111 11111111 11111111 00000000	255. 255. 255. 0	/24

- The mask can help to find netid and the hostid. For example, the mask for class A address has eight 1s, which means the first 8 bits of any address in class A define the netid, the next 24 bits define the hostid.
- The last column of Table 5.2 shows the mask in the form /n where n can be 8, 16 or 24 in classful addressing. This notation is also called **slash notation** or **Classless Inter-Domain Routing (CIDR)**.

5.2.3 Classless Addressing

- To solve the address depletion problem and give more organizations access to the Internet, classless addressing was designed and implemented. No classes are used but the addresses are still granted in blocks.

Address Blocks:

- In classless addressing, when a computer or number of computers or any device needs to be connected to the Internet, an ISP (Internet Service Provider) grants a block (range) of addresses.
- The size of block i.e., number of addresses varies based on the nature and number of computers (entity). For example, a single home user may require one address whereas an organization may require more.
- An ISP may be given thousands or hundreds of thousands addresses based on the number of customers it may serve.
- To make it simple, the Internet authorities impose three restrictions on classless address blocks:
  1. The addresses in a block must be contiguous, one after another.
  2. The number of addresses in a block must be a power of 2 (1, 2, 4, 8, 16, ...).
  3. The first address must be evenly divisible by the number of addresses.
- Fig. 5.6 shows blocks of 16 addresses granted to a small business.

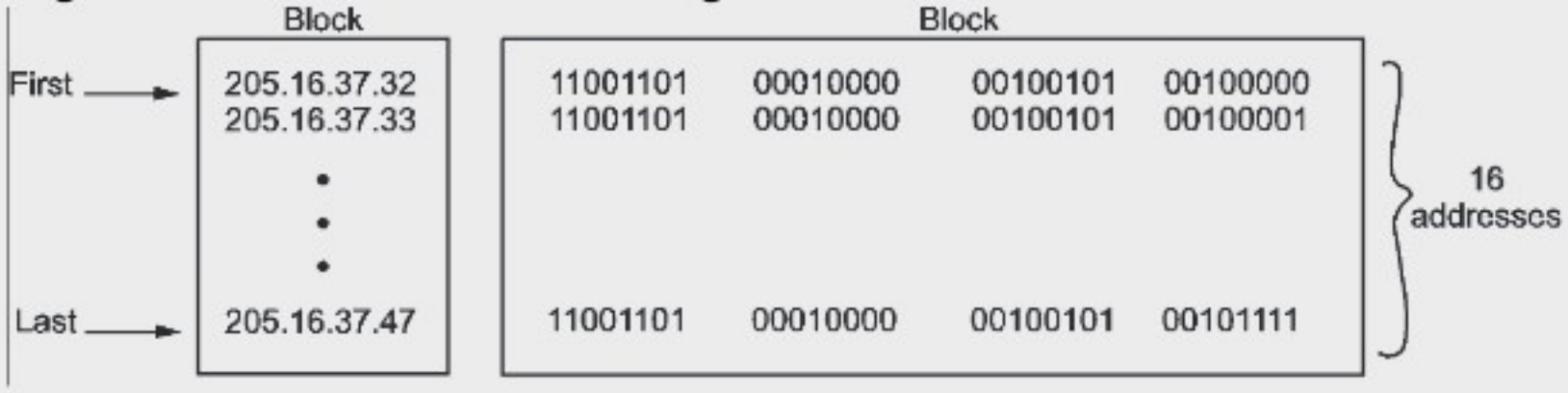


Fig. 5.6: A Block of 16 Addresses Granted to a Small Organization

- From the Fig. 5.6, we can say that all the addresses are contiguous. The number of addresses are 16 which is power of 2. The first address, when converted to a decimal number is 3, 440, 387, 360 which is evenly divisible by 16.

Mask:

- To define a block of addresses is to select any address in the block and the mask.
- The mask is a 32 bit number in which the n left most bits are 1s and the 32-n rightmost bits are 0s.
- In IPv4 addressing, a block of addresses can be defined as x.y.z.t/n, where x.y.z.t defines one of the addresses and the /n defines the mask.
- The addresses and the /n notation completely define the whole block, (the first address, the last address and the number of addresses).

First Address:

- The first address in the block can be found by setting the right most 32-n bits to 0s.
- For example: A block of addresses is granted to a small organization. We know that one of the addresses is 205.16.37.39/28. What is the first address in the block?

  The binary representation of the given address is:

  11001101 00010000 00100101 00100111.

  If we set 32 – 28 rightmost bits to 0, we get,

  11001101 0001000 00100101 00100000,

  Which is represented as 205. 16. 37. 32, is the first address.

Last Address:

- The last address in the block can be found by setting the right most 32 – n bits to 1s.

  For example: Find the last address for the block 205. 16. 37. 39/28.

  The binary representation of a given address is:

  11001101 00010000 00100101 00100111.

  If we set 32 – 28 = 4 rightmost bits to 1, we get,

  11001101 00010000 00100101 00101111, which is represented in binary as 205.16.37.47 is a last address.

Number of Addresses:

- The number of addresses in the block can be found by using the formula 2^{32-n}.
- For example: Find the number of addresses in 205.16.37.39/28 used in the address block.

  Here, $n = 28$

  $\therefore \quad 2^{32-n} = 2^{32-28}$

  $= 2^4$

  $= 16$

  The number of addresses are 16.

Network Addresses:

- In IP addressing, the network address concept is used. When a block of addresses are allocated to an organization, it is free to allocate the addresses to the devices that need to be connected to the Internet.
- The first address in the block is normally not assigned to any device, it is used as the network address that represents the organization to the rest of the world. Rest of the world identifies that network by first address.
- From Fig. 5.7, we can say the organization network is connected to the Internet via a router. The router has two addresses one for organization network and one for rest of the word, i.e. the addresses 205.16.37.40/28 and x.y.z.t/n. All messages are designed

for addresses in the organization block (205.16.37.32 to 205.16.37.47) are sent to x.y.z.t/n.

- The first address in a block is normally not assigned to any device, it is used as the network address that represents the organization to the rest of the world.

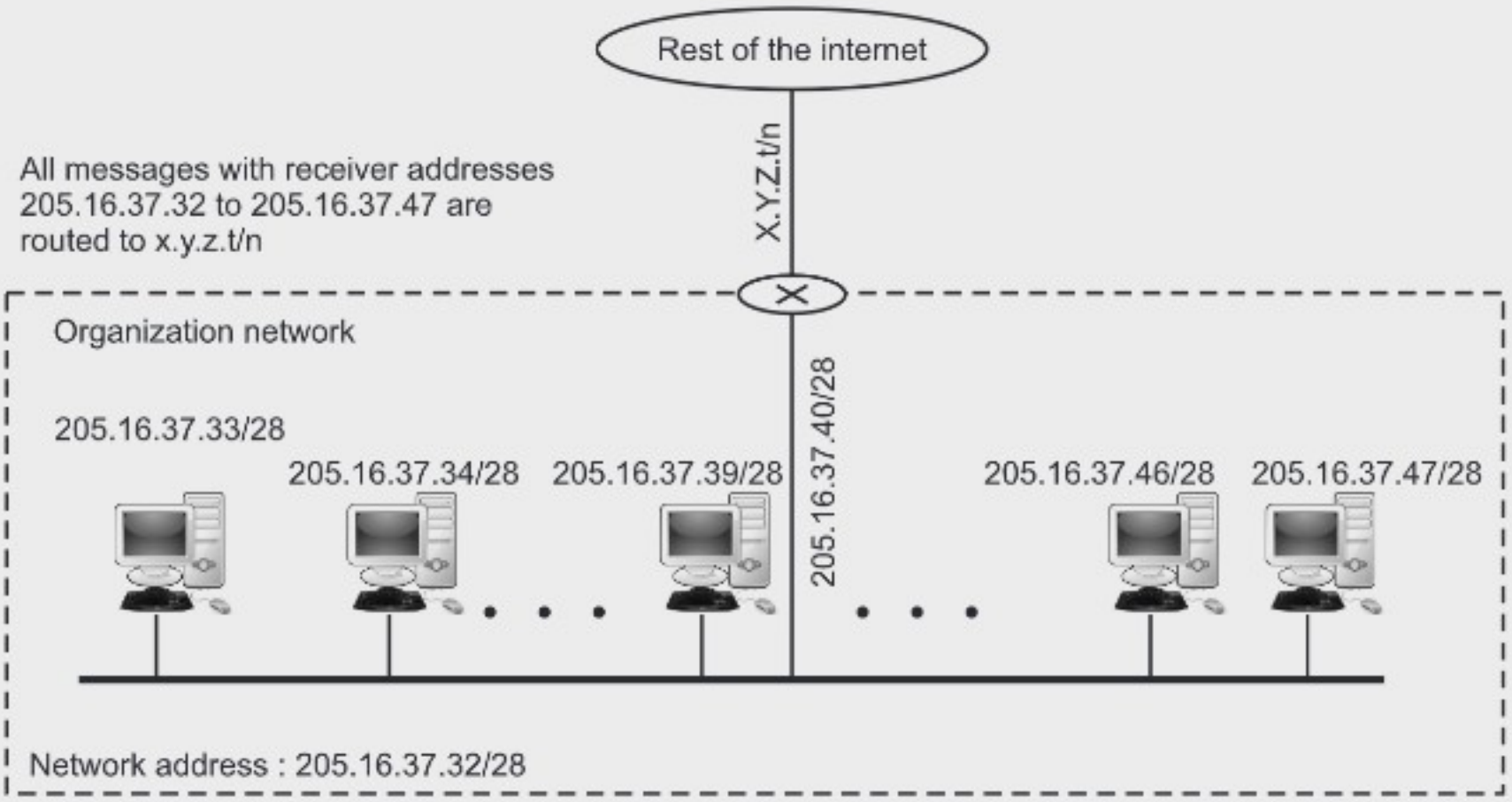


Fig. 5.7: A Network Configuration for the Block 205.16.37.32/28

Hierarchy:

- IP addresses like any other identifiers, have levels of hierarchy.
- For example: A phone number 02025512336 is having STD code first, then area code and phone number.

Two-Level Hierarchy: No Subnetting:

- When not subnetted, IP address defines two levels of hierarchy. Each address in the block can be considered as a two-level hierarchical structure, the leftmost n bits (prefix) define the network; the rightmost 32-n bits define the host.
- Fig. 5.8 shows two levels of hierarchy in an IPv4 address.

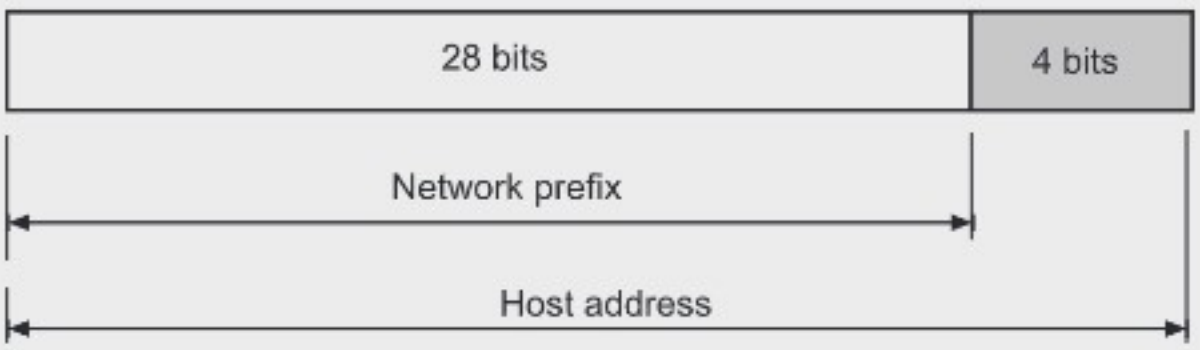


Fig. 5.8: Two Levels of Hierarchy in an IPv4 Address

Three-Levels of Hierarchy: Subnetting:

- An organization which is granted a large block of address creates small networks subnets. All available addresses are distributed among these subnets.
- For the rest of the world, the organization is still identified by one IP address, however internally there are several subnets. All messages are sent to the router address that connects the organization to the rest of the Internet.
- The router routes the messages to the appropriate subnet. Small subblocks of addresses are assigned to specific subnets. The organization and it's subnets have its own mask.
- Consider, as an example an organization is given the block 17.12.40.0/26, which contains 64 addresses. The organization has three offices and needs to divide the addresses into three subblocks of 32,16, and 16 addresses.
- We can find the new masks by using:
  1. Suppose the mask for the first subnet is n1, then 2^{32-n1} must be 32, which means that $n^1 = 27$.
  2. Suppose the mask for the for the second subnet is n2, then 2^{32-n2} must be 16, which means that $n^2 = 28$.
  3. Suppose the mask for the third subnet is n3, then 2^{32-n3} must be 16, which means that $n^3 = 28$.
- We have the mask 27, 28, 28 with the organization mask being 26. Fig. 5.9 shows this configuration.

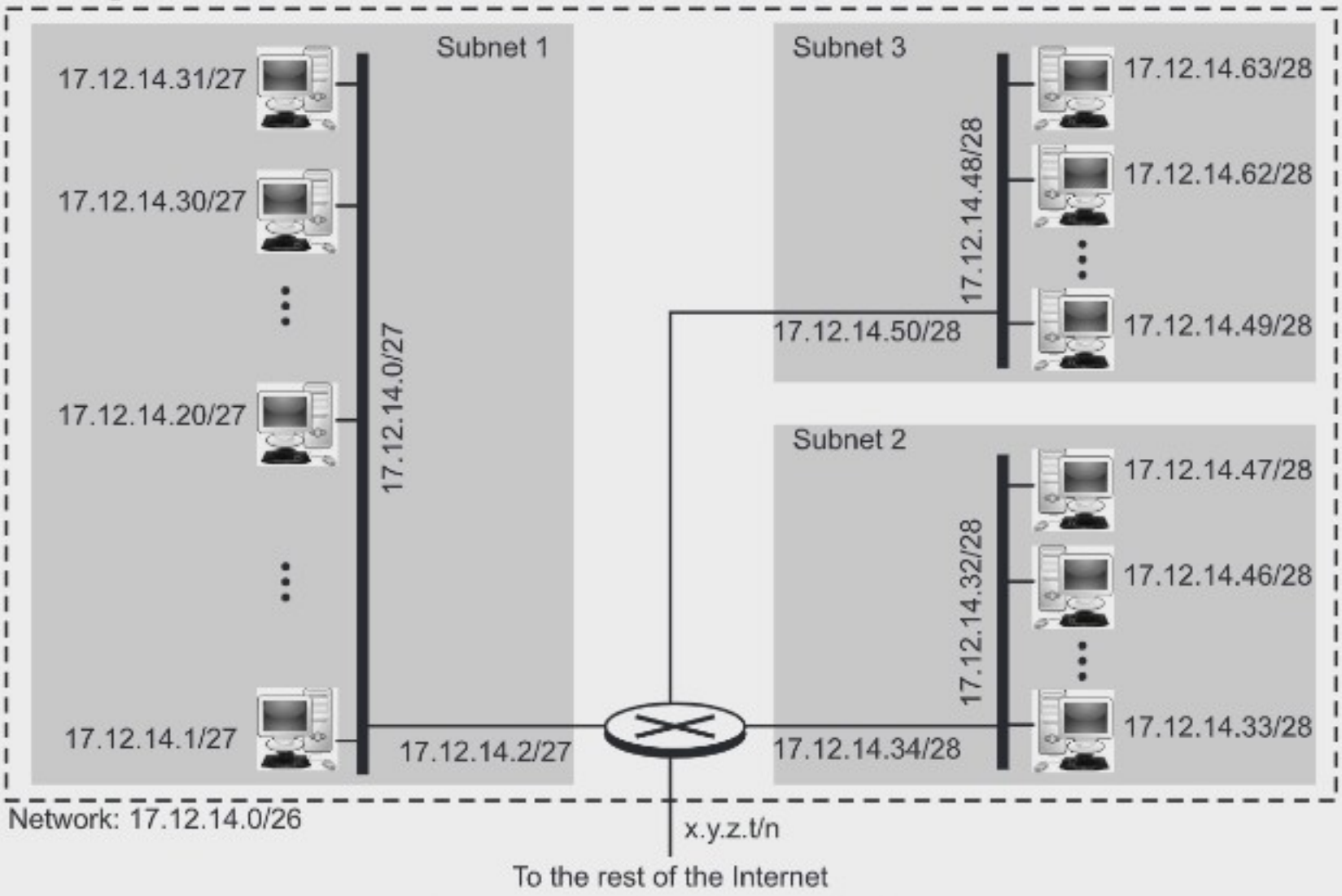


Fig. 5.9: Subnetting in Organization

- Through subnetting, we have three levels of hierarchy. It is shown in the Fig. 5.10.

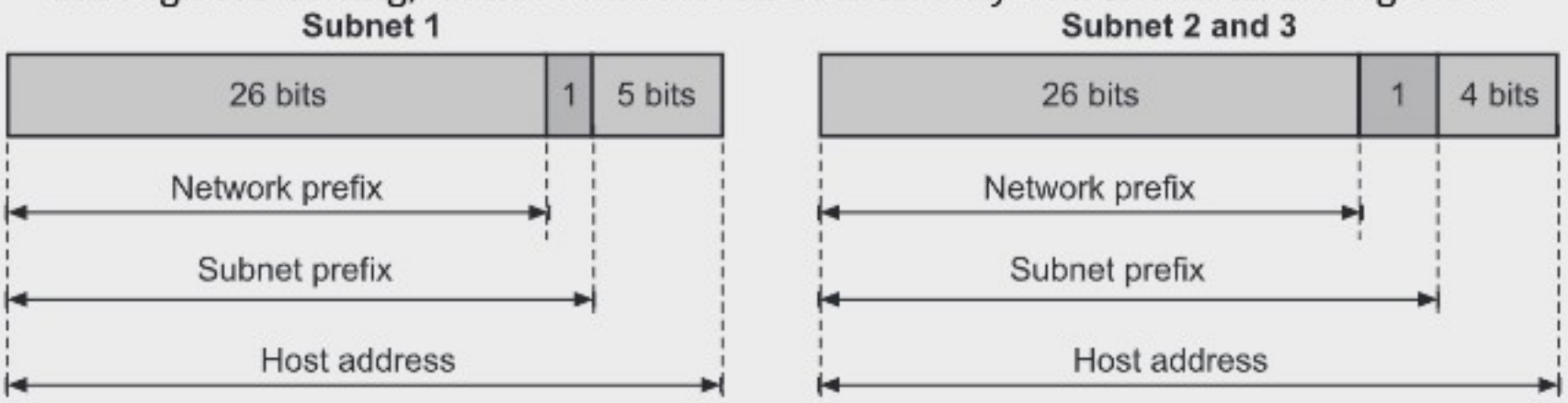


Fig. 5.10: Three Levels of Hierarchy

More Levels of Hierarchy:

- In classless addressing the number of hierarchical levels are not restricted.
- An organization can divide the granted block of addresses into subblocks. Each subblock is further subdivided into smaller subblocks, and so on.

Address Allocation:

- The responsibility of address allocation is given to a global authority called the Internet Corporation for Assigned Names and Addressed (ICANN).
- ICANN assigns a large block of addresses to an ISP. This large block is distributed to it ISP's customers. This is called address aggregation: many blocks of addresses are aggregated in one block and granted to one ISP.

5.2.4 Network Address Translation (NAT) (W-18)

- The number of home users and small businesses who want to use the Internet is day-by-day increasing. In earlier days, users were connected to the Internet for specific time by dial-up lines.
- ISP assigns a block of addresses to its user. An address is assigned to a user when it is needed.
- Today dial-up connections are not that much used. Home users and small businesses can be connected by ADSL lines (Broadband) or cable modem with high speeds.
- Additionally users require more addresses for their small networks. With the shortage of addresses, this is a serious problem. A solution to this problem is Network Address Translation (NAT).
- With NAT, a user uses a large set of addresses internally and only one or small set of addresses for the outside world.
- To separate the addresses used inside and outside the Internet authorities reserved three sets of addresses as private addresses. These are given in Table 5.3.

Table 5.3: Addresses for private networks

Range	Total
10.0.0.0 to 10.255.255.255	2^{24}
176.16.0.0 to 172.31.255.255	2^{20}
192.168.0.0 to 192.168.255.255	2^{16}

- All the addresses shown in the above Table 5.3 are unique inside the organization, but they are not unique globally. Any organization can use these addresses without permission from the Internet authorities.
- Out of these addresses, if any address is used as a destination address, the router will not forward such packets.
- Fig. 5.11 shows a simple implementation of NAT.

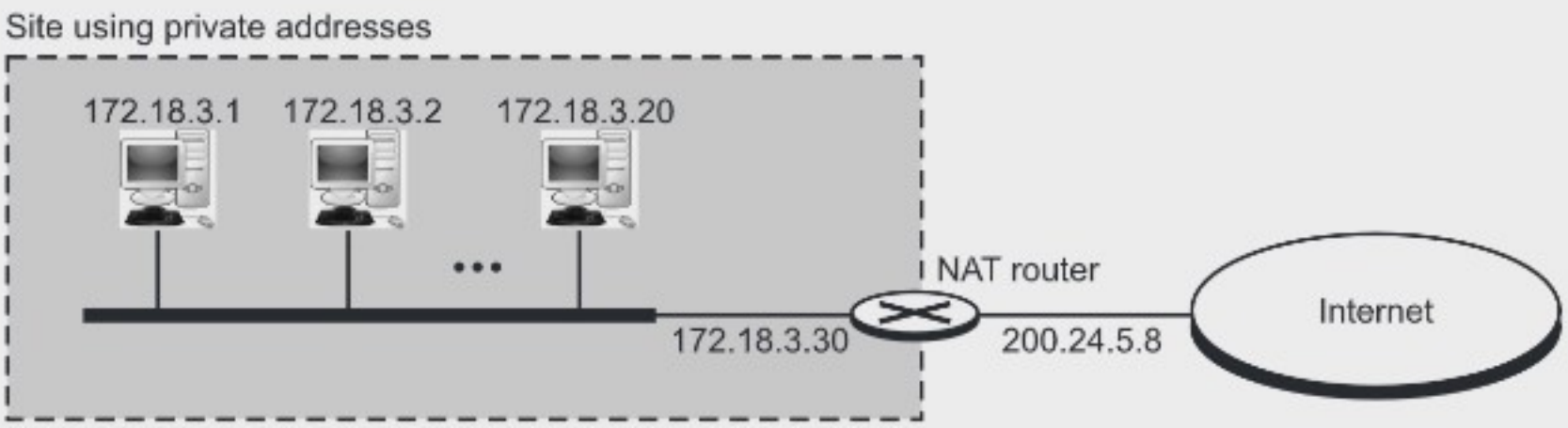


Fig. 5.11: A NAT Implementation

- Fig. 5.11 shows the private network using private addresses. The router that connects the network to the global address uses one private address and one global address.
- The private network is transparent to the rest of the Internet. The rest of the Internet sees only NAT routers with the address 200.24.5.8.

Address Translation:

- Fig. 5.12 shows an example of address translation.

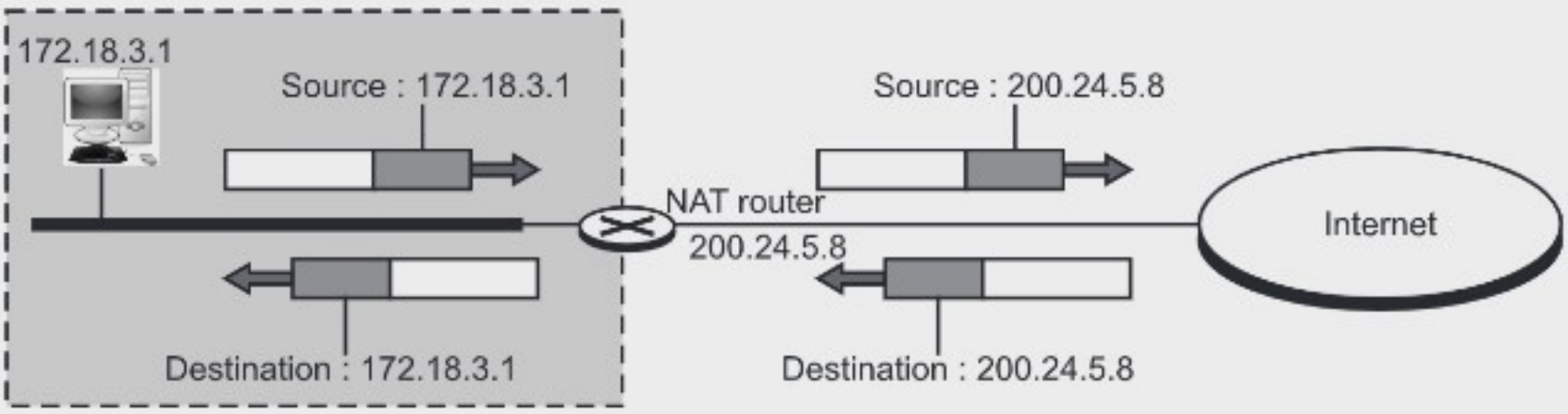


Fig. 5.12: Addresses in NAT

- Each outgoing packet goes through a NAT router, which replaces the source address in the packet with global NAT address.
- Each incoming packet also passes through the NAT router, which replaces the destination address in the packet with the appropriate private address.

Translation Table:

- When packets are going from the network, address translation is very simple.
- Only the source address of the packet is changed and NAT router's address is assigned. But when packets are coming from the Internet with the destination address of a NAT router, how does the NAT router know the destination address to deliver it.

- Because there may be tens or hundreds of private IP addresses, each belonging to one specific host. To solve this problem NAT router using a translation table.

1. Using One IP Address:

- A translation table has only two columns i.e., the private address and the external address (destination address for a packet).
- Router makes a note of the source address of the outgoing packet. It also makes note of the destination address where the packet is going.
- When the response comes back from the destination, the router uses the source address of the packet (as the external address) to find the private address of the packet. Fig. 5.13 shows this concept.

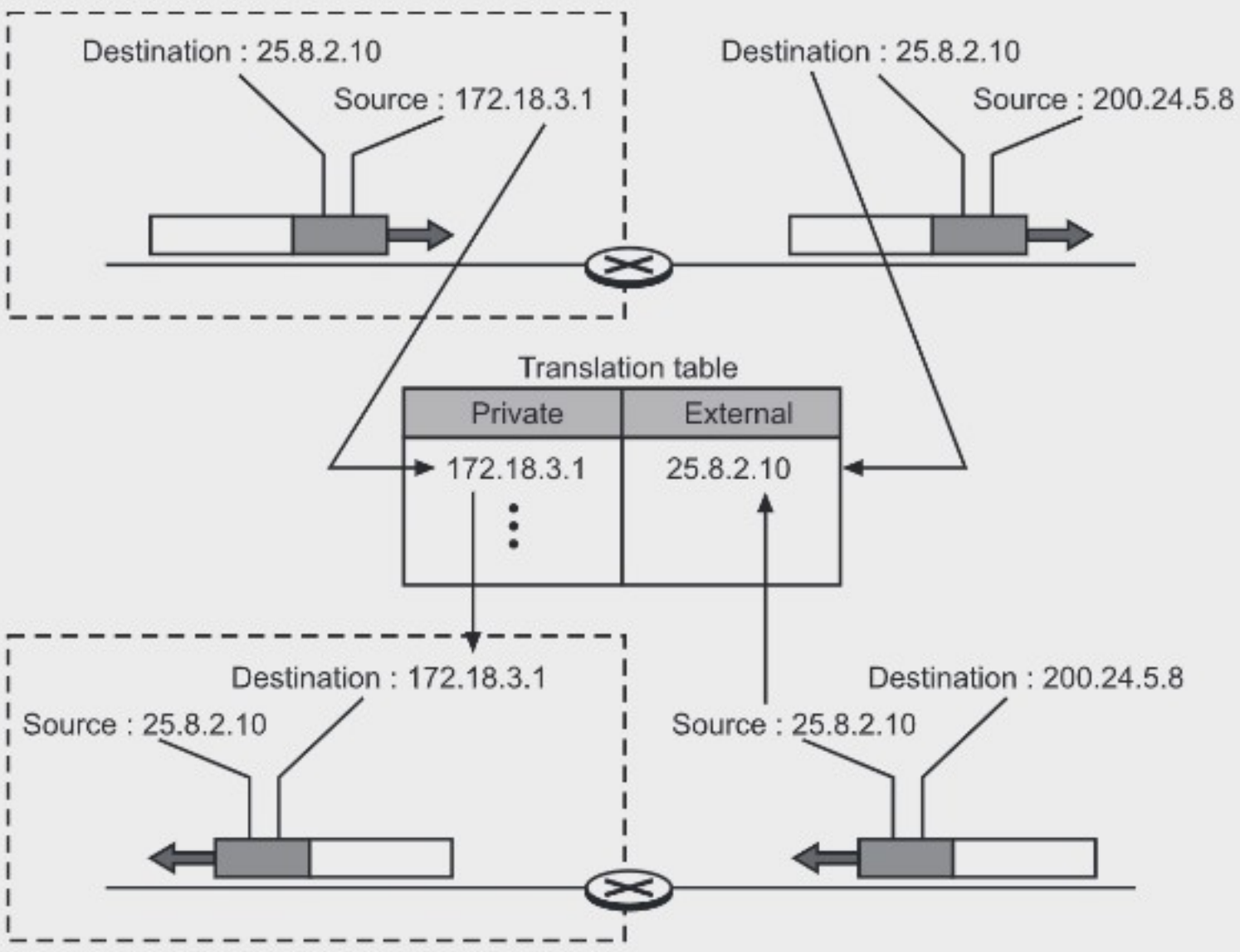


Fig. 5.13: NAT address Translation using One IP Address

- Note that in this strategy, communication must be initiated by a private network. NAT is mostly used by ISPs. ISPs assign a single address to its customer, which may use a number of private addresses. Generally communication with the Internet is always initiated by customers.

2. Using a Pool of IP Addresses:

- NAT router has only one global address, only one private network host can access the same external host. To remove this drawback, the NAT router uses a pool of global addresses.

- For example, instead of using only one global address (200.24.5.8), the NAT router can use four addresses (200.24.5.8, 200.24.5.9,200.24.5.10, and 200.24.5.11). In this case, four private network hosts can communicate with the same external host at the same time because each pair of addresses defines a connection.

3. Using Both IP Addresses and Port Numbers:

- To allows a many-to-many relationship between private-network hosts and external server programs, more information in the translation table is required.
- For example, suppose two hosts with addresses 172.18.3.1 and 172.18.3.2 inside a private network need to access the HTTP server on external host 25.8.3.2. If the translation table has five columns, instead of two, that include the source and destination port numbers of the transport layer protocol, the ambiguity is eliminated.
- Table 5.4 shows an example of such a table.

Table 5.4: Five-column translation table

Private Address	Private Port	External Address	External Port	Transport Protocol
172.18.3.1	1400	25.8.3.2	80	TCP
172.18.3.2	1401	25.8.3.2	80	TCP
...	...	...	...	...

NAT and ISP:

- Suppose an ISP is granted 1000 addresses, but has 10,000 customers. Every customer is assigned a private network address.
- The ISP translates every 10,000 source addresses in outgoing packets to one of the 1000 global addresses. It translates the global destination address in incoming packets to the corresponding private address, (See Fig. 5.14).

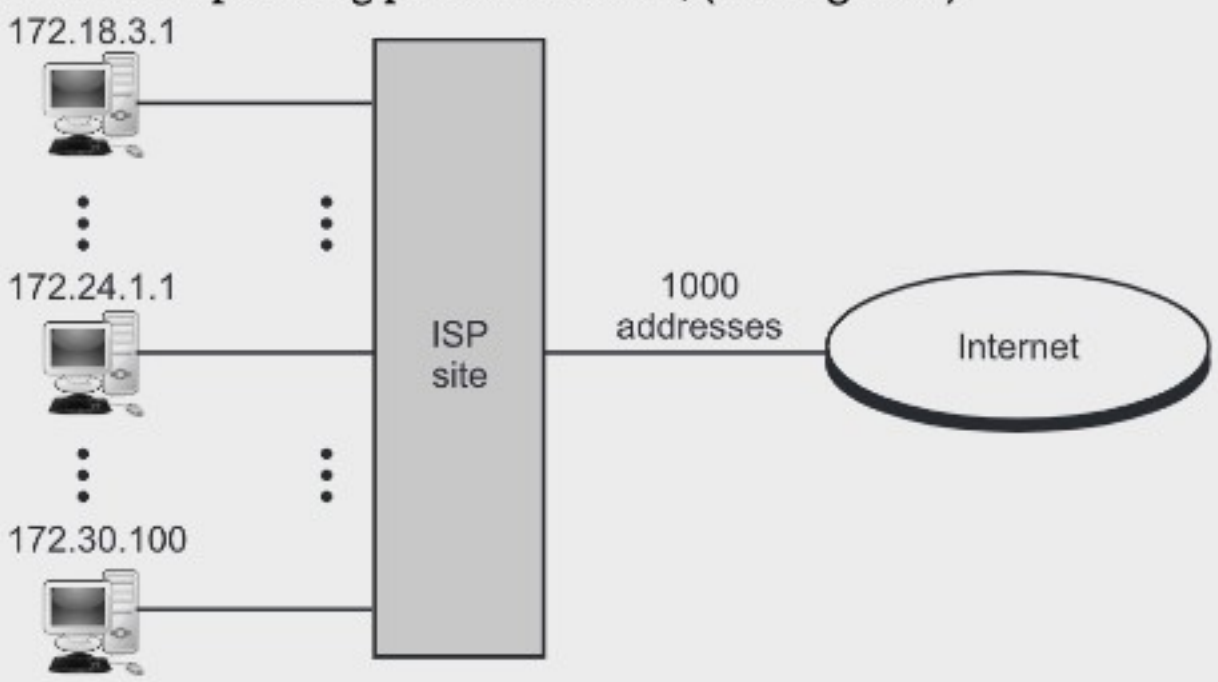


Fig. 5.14: An ISP and NAT

5.2.5 Subnetting (W-18)

- If an organization was granted a large block in class A or B, it could divide the addresses into several continuous groups and assign each group to smaller networks (called subnets).
- The subnets are created through the use of subnet masks. The subnet mask identifies which bits in the IP address are to be used to represent the network/subnet portion of an IP address.
- Subnetting is "the process of dividing (partitioning) a network into several smaller networks (subnets)".

5.2.6 Supernetting (S-19, 18; W-18)

- When most of the class A and class B addresses were depleted, there was a huge demand for midsize blocks. The size (only 256) of class C was not sufficient. Even a midsize organization needs more than 256 addresses. Super netting is solution for this problem.
- In supernetting, an organization can combine several class C blocks to create a larger range of addresses.
- Several networks are combined to create a supernetworks or a supernet.

Address Depletion:

- Since the drawbacks in classful addressing and the Internet is growing very fastly, shortage of available addresses comes into picture.
- The continuous and fast growth of Internet led to the shortage of the available addresses. Yet the number of devices on the Internet is much less than the 232 address space. We have run out of class A and class B addresses, and class C block is too small for most mid-size organizations.
- One solution for this problem is idea of classless addressing. Classful addressing, which is almost obsolete, is replaced with classless addressing.

5.3 IPV4 PROTOCOL

- Internet Protocol version 4 (IPv4) is the fourth revision of the IP and a widely used protocol in data communication over different kinds of networks as a delivery mechanism.
- Fig. 5.15 shows the position of IPv4 in the Internet model.
- IPv4 protocol has the responsibility of identifying hosts based upon their logical addresses and to route data among them over the underlying network.
- IPv4 is an unreliable and connectionless datagram protocol, which does not provide error control or flow control mechanisms (except for error detection on the header). IP is also called the best effort delivery protocol.

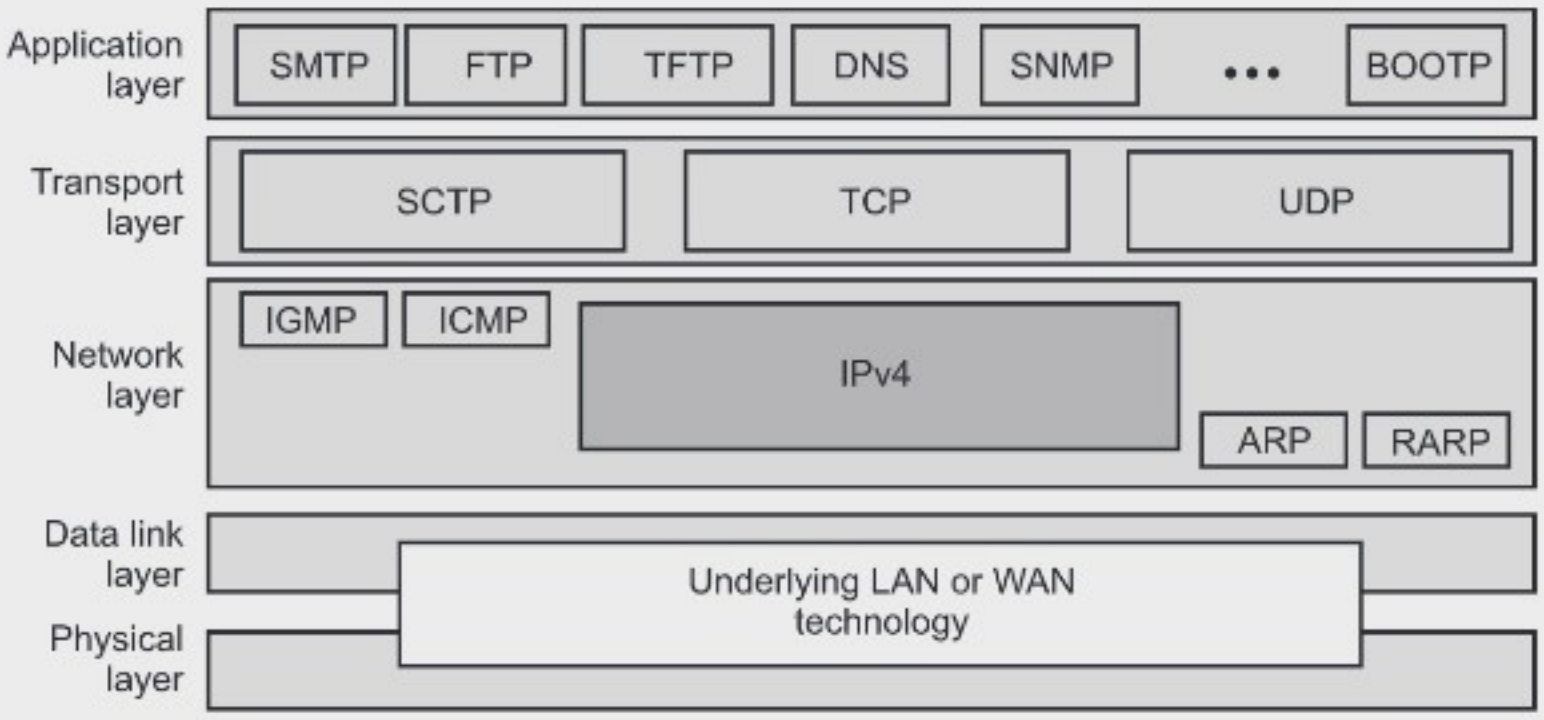


Fig. 5.15: The Position of IPv4 in the Internet Model

- For example, the post office. Post office does its best to deliver the mail but does not always succeed and does not take any guarantee of delivery. If an unregistered letter is lost, the post office does not inform the original sender about loss or damage.
- IP is also done the same, if a datagram is lost or damaged, IP will not inform the original sender and the damaged datagram is simply discarded.
- IPv4 is a connectionless protocol for a packet switched network. Datagrams sent by the same source to the same destination could arrive out of order. IPv4 relies on the higher layer for reliability.

5.3.1 IP Datagram (S -18)

- In IPv4, packets are called datagram, which is a basic transfer unit associated with a packet-switched network.
- The delivery, arrival time, and order of arrival need not be guaranteed by the network.
- Fig. 5.16 shows IPv4 datagram format.
- A datagram is a variable length packet which contains two parts i.e., header and data. The header is in between 20 to 60 bytes in length and contains information required for routing and delivery.

Fields in IPv4 Datagram: (S-19)

1. **Version (VER):** This 4 bit field defines the current version of IPv4. Currently the version is 4. This field tells the IPv4 software running in the processing machine that the datagram has format of version 4 and all fields must be treated as version 4.

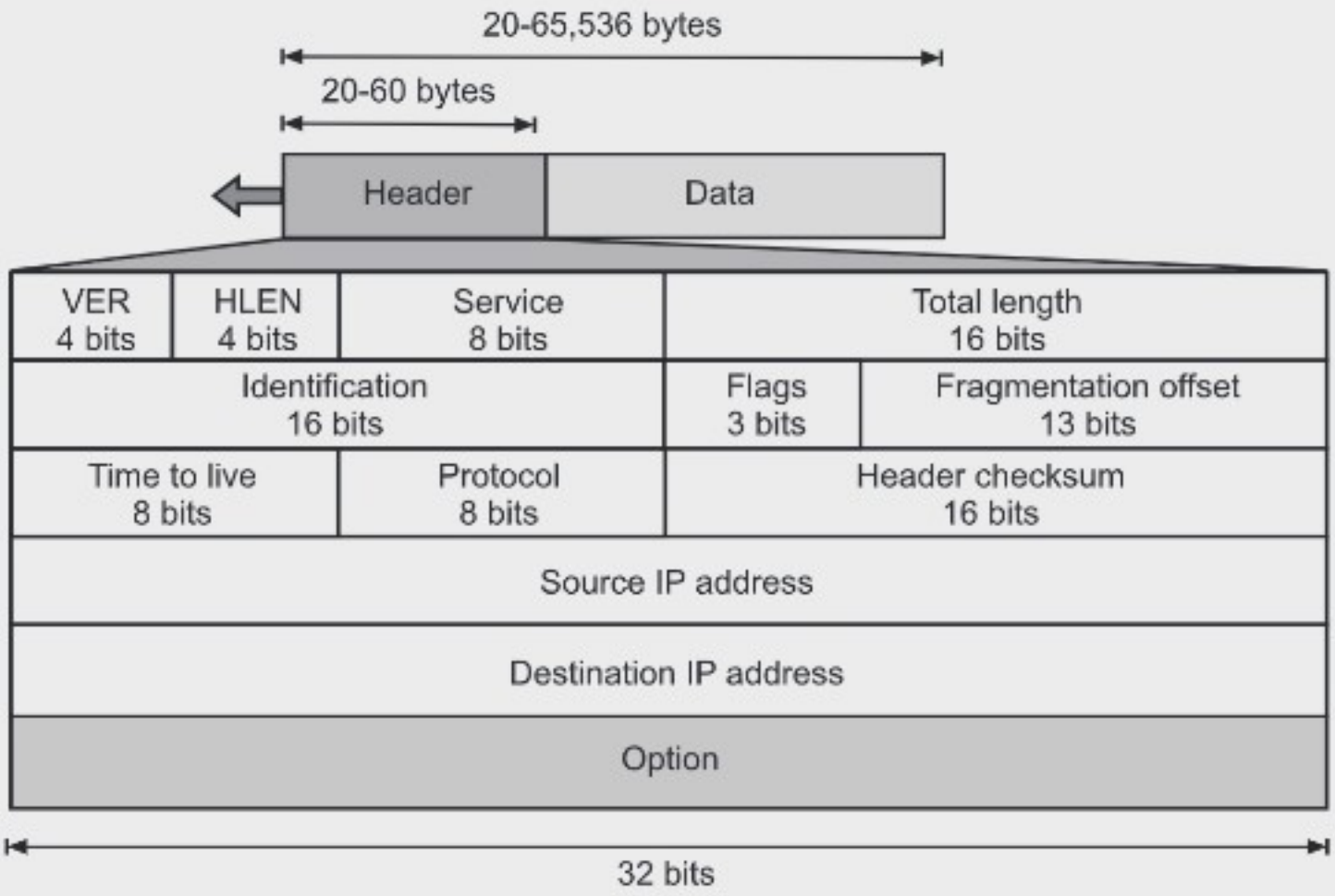
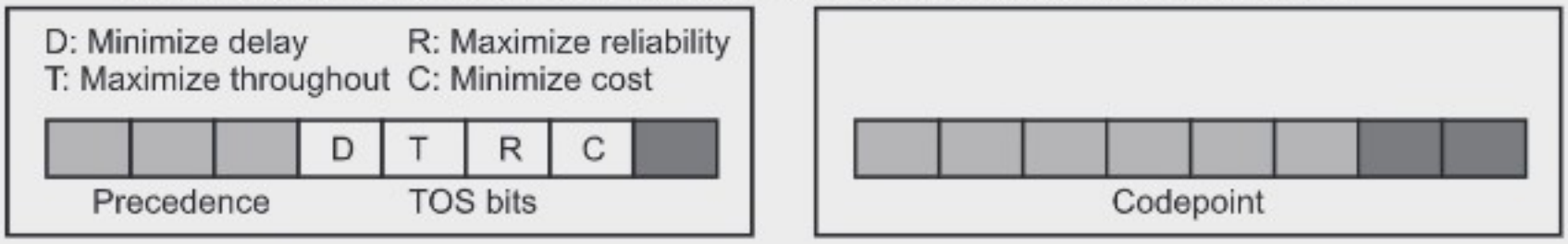


Fig. 5.16: IPv4 Datagram Format

2. **Header Length (HLEN):** This 4 bit field defines the total length of the header. The length of the header is variable (between 20 to 60 bytes). When there are no options, the header length is 20 bytes, and value is 5 (5 × 4 =20). When option field is at its maximum size, the value of this field is 15 (15 × 4 = 60).
3. **Services:** This 8 bit field previously known as service type, is now called differentiated services. Both implementations are shown in Fig. 5.17.



(a) Service Type **(b) Differentiated Services**

Fig. 5.17

(i) **Service type:** First 3 bits are called precedence bits, the next 4 bits are Type Of Services (TOS) bits and the last bit is not used.

(a) **Precedence:** This three bit subfield ranging from 0(000 in binary) to 7(111 in binary). This field defines priority of the datagram in issues such as congestion. If a router is congested, it discards some datagrams. Datagrams with the lowest priority are discarded first.

(b) **TOS Bits:** This 4 bit subfield defines types of services. We can have 5 different types of services as listed in the following table.

Table 5.5: Types of Services

TOS Bits	Description
0000	Normal (default)
0001	Minimize cost
0010	Maximize reliability
0100	Maximize throughput
1000	Minimize delay

(ii) **Differentiated services:** The first 6 bits made the codepoint subfield, and the last 2 bits are not used.

4. **Total length:** This 16 bits field defines the total length of the datagram including the header. IPv4 datagram maximum size is 65,535, of which 20 to 60 bytes are the header and the rest is data from the upper layer.

   Length of data = Total length – Header length

5. **Identification:** This field is used in fragmentation.
6. **Flags:** This field is used in fragmentation.
7. **Fragmentation Offset:** This field is used in fragmentation.
8. **Time to live:** This field is used to control the maximum number of hops (routers) visited by the datagram since every datagram has a limited lifetime to travel through an internet. When a source sends a datagram, it stores a number in this field. This value is approximately double the maximum number of routes between any two hosts. Every time datagram visits a router, router decrements this number by 1. If this value, after being decremented, is zero, the router discards the datagram assuming the datagram lost the route.

   On the Internet, routing tables of routers may be corrupted. A datagram may travel between two or more routers for a long time without being delivered to the destination. This field limits the lifetime of a datagram.

   This field also limits the journey of the packet. For example, if a source wants that packet should not leave the home network, then it can store 1 in this field. When the packet arrives at the first router, this value is decremented to 0 and the datagram is discarded.

9. **Protocol:** This 8 bit field defines the higher level protocol that uses the services of IPv4. IPv4 protocol carries data from different other protocols(TCP, UDP, ICMP, etc.), the value of this field helps the receiving network layer know to which protocol the data belong.
10. **Checksum:** This field is used for error detection.
11. **Source address:** This 32 bit field defines the source address of a datagram.
12. **Destination address:** This 32 bit field defines the destination address of a datagram.

5.3.2 Fragmentation

- Now, we will discuss fragmentation of IPv4 datagram in detail.
- To reach upto destination, datagram may travel through different networks. Every router decapsulates the IPv4 datagram from the frame it receives, processes it, and then encapsulates it in another frame.
- The format and size of a frame depends upon the type of a network. Two networks may have different frame formats and different sizes.
- For example: If a router connects a LAN to a WAN, it receives a frame in the LAN format and sends a frame in the WAN format.
- Each data link layer protocol has its own frame format in most protocols. Maximum Transfer Unit (MTU) defines the maximum size of the data field. The value of the MTU depends on the physical network protocol.

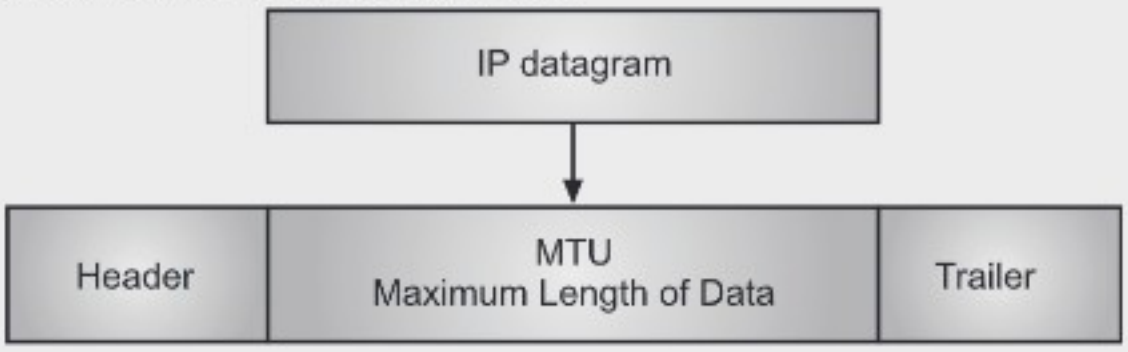


Fig. 5.18: Maximum Transfer Unit (MTU)

Table 5.6: MTU for Some Networks

Protocol	MTU
Hyperchannel	65,535
Token ring (16 mbps)	17,914
Token ring (4 mbps)	4,464
FDDI	4,352
Ethernet	1,500
X.25	576
PPP	296

- To make the IPv4 protocol independent of the physical network, length of IPv4 datagram equal to 65,535 bytes. This makes a transmission more efficient if we use a protocol with an MTU of this size. However, for other physical networks, we must divide the datagram, so that it can pass through these networks. This is called fragmentation.
- When a datagram is fragmented, every fragment has its own header. Most of the fields are repeated and some are changed in fragments. A fragmented datagram can be fragmented if required. A datagram can be fragmented several times before it reaches the final destination.

- In IPv4, datagram can be fragmented by the source or routers in the path. But reassembly of datagram is done only by the destination host. Because every fragmented datagram may be routed independently by different routes and we can never control or guarantee which route a fragmented datagram may take. All these fragments arrive at the destination host. So the reassembly is done at the final destination.
- The host or router that fragments a datagram must change the values of three fields i.e., Flags, fragmentation offset and total length. Other fields are copied as it is.

Fields Related to Fragmentation:

- The fields related to fragmentation are identification, flags and fragmentation offset. These fields are described below.

1. **Identification:**

- This 16 bit field identifies a datagram originating from the source host. Identification and source address uniquely defines a datagram as it leaves the source host. For uniqueness, IPv4 protocol uses a counter.
- When datagram is sent, IPv4 copies the current value of the counter to the identification field and increments the counter by 1.
- When a datagram is fragmented, this value is copied to all fragments so that all fragments have the same identification number. This identification number helps the destination host at the time of reassembly.

2. **Flags:**

- There are 3 bits in flag, From the 3 bits the first bit is reserved.
- The second bit is called the do not fragment bit. If its value is 1, the machine must not fragment the datagram. If it cannot pass the datagram, it must discard it. If the value is 0, the datagram can be fragmented if necessary.
- The third bit is called the more fragment bit. If its value is 1, means the datagram is not the last fragment, more fragments are coming after this. If its value is 0, it means this is the only or last fragment.

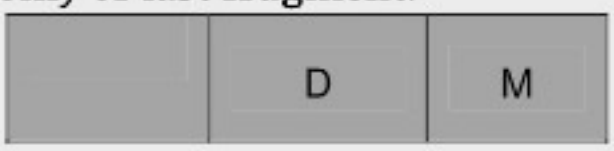


Fig. 5.19: Flags used in Fragmentation

3. **Fragmentation Offset:**

- This 13 bit field shows the position of the fragment with respect to the whole datagram.
- Fig. 5.20 shows a datagram with a data size of 4000 bytes fragmented into three fragments.
- The bytes in the original datagram are 0 to 3999. The first fragment carries 0 to 1399 bytes. The offset for this datagram is = 0. The second fragment carries 1400 to 2799, the offset is = 8 = 175. The third one carries 2800 to 3999 bytes. The offset value is = 350.

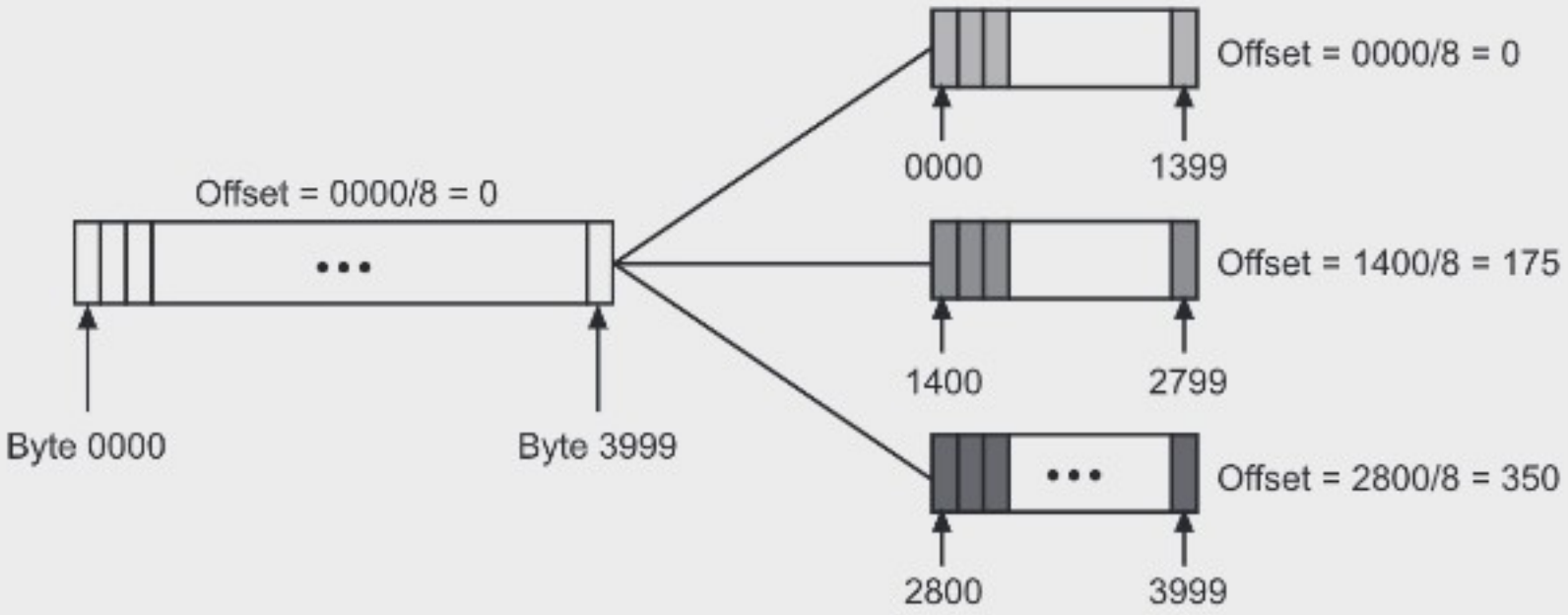


Fig. 5.20: Fragmentation Example

- Fig. 5.21 shows an expanded view of the fragments in Fig. 5.20.

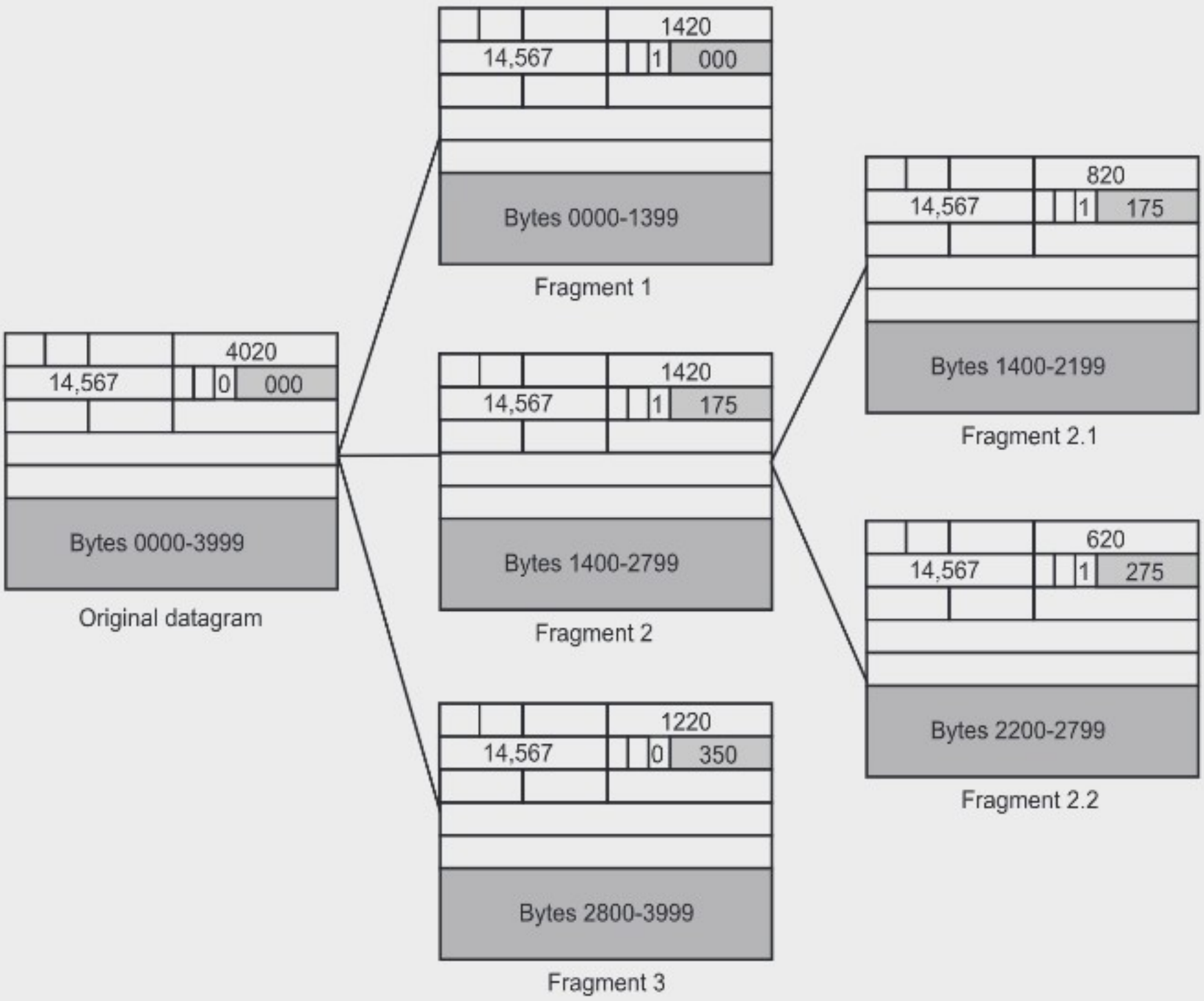


Fig. 5.21: Detailed Example

5.3.3 Checksum (S -19)

- To compute checksum in IPv4, the value of the checksum field is set to 0. Then the entire header is divided into 16 bit sections and added together. The result (sum) is complemented and inserted into the checksum field.
- The checksum covers only the header, not the data.
- Fig. 5.22 shows an example of a checksum calculation for IPv4 header without options.
- The header is divided into 16 bit sections. All the sections are added and the sum is complemented. The result is inserted in the checksum field.

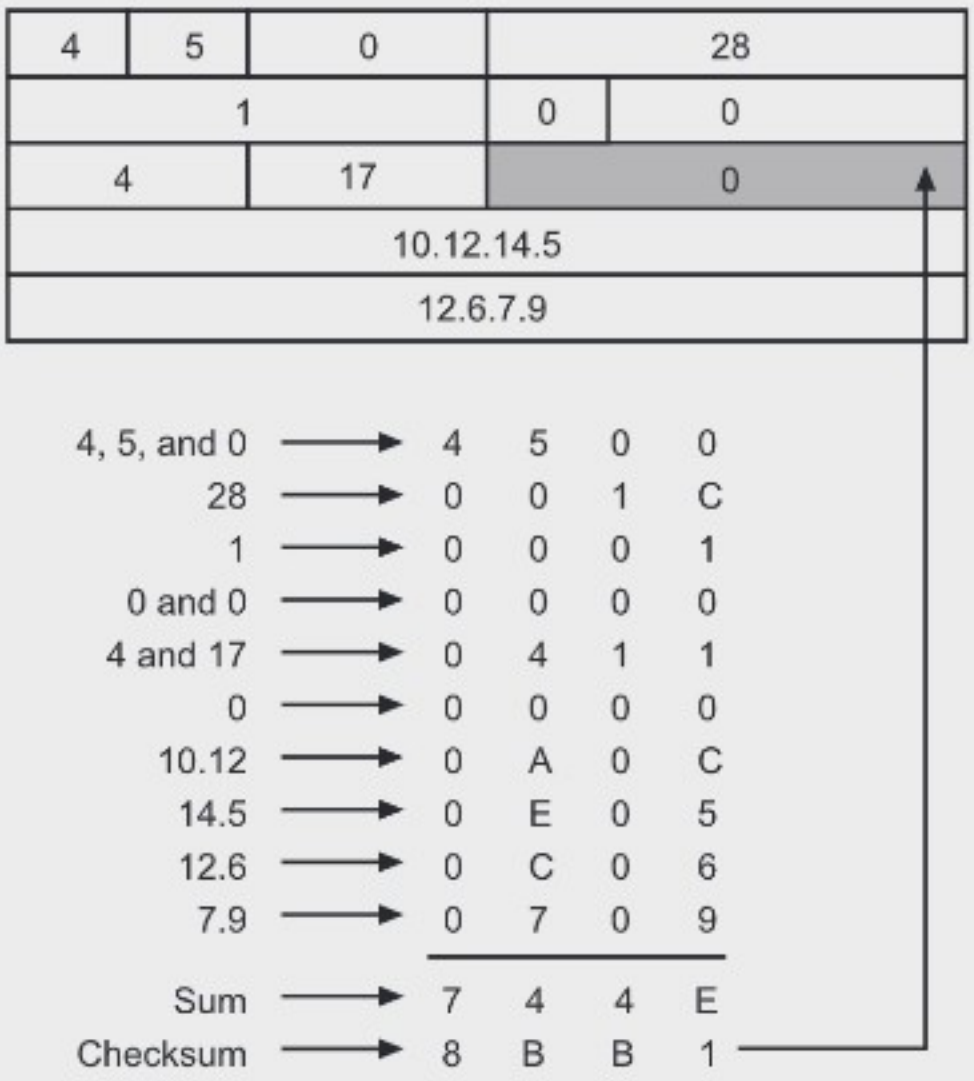


Fig. 5.22: Example of checksum Calculation of IPv4

5.3.4 Options

- The header of IPv4 datagram is of two parts i.e., Fixed part and Variable part.
- The fixed part is 20 bytes long and the variable part is maximum of 40 bytes.
- Options are not required for a datagram, they are used for network testing and debugging.
- Fig. 5.23 shows types of options.

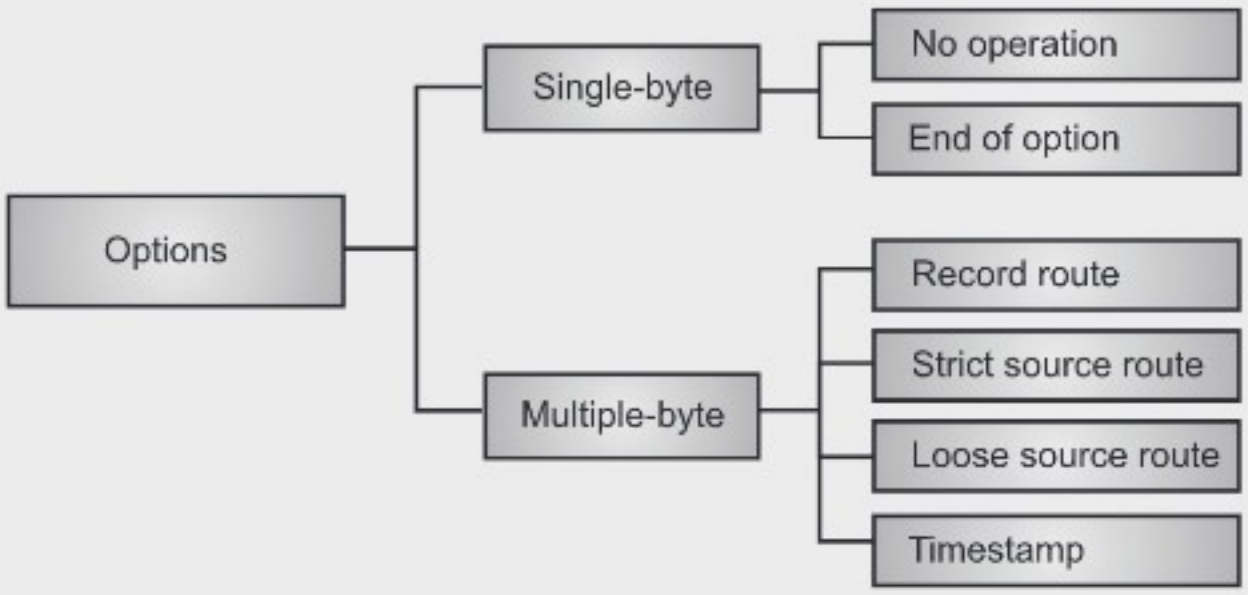


Fig. 5.23: Options in IPv4

- Various options in IPv4 are listed below:
  1. **No Operation:** A no-operation option is a 1 byte option used as a filler between options.
  2. **End of Option:** An end-of-option is a 1 byte option used for padding at the end of the option field. It can only be used as the last option.
  3. **Record Route:** A record route option is used to record the Internet routers that handle the datagram. It can list upto nine router addresses.
  4. **Strict Source Route:** A strict source route option is used by the source to predetermine a route for the datagram as it travels through the Internet. The sender can choose a route with a specific type of service (e.g. minimize delay, maximum throughput). If a datagram specifies a strict source route, all the routers defined in the option must be visited by the datagram. If an address of a router is not mentioned in the route list, it must not be visited. If datagram visits a route that is not on the list, datagram is discarded. If datagram arrives at the destination and some of the entries were not visited, it will be also discarded.
  5. **Loose Source Route:** A loose source route option is similar to strict source route. Only one difference is, each router in the list must be visited, but the datagram can visit other routers also.
  6. **Timestamp:** A timestamp option is used to record the time of datagram processing by a router. This can help users and managers to track the behaviour of the routers on the Internet. We can estimate time taken for a datagram to go from one router to another.

Example 3: A packet has arrived with an m bit value of 0. Is this the first fragment, the last fragment, or a middle fragment ? Do we know if the packet was fragmented ?

Solution: If the m bit is 0, it means there are no more fragments, the fragment is the last one. We cannot say if the original packet was fragmented or not. A non-fragmented packet is considered the last fragment.

Example 4: A packet has arrived with a m bit value of 1. Is this the first fragment, the last fragment or middle ?

Solution: If the m bit is 1, it means that there is atleast one or more fragments. This fragment can be the first one or the middle one, but not the last one.

Example 5: A packet has arrived in which the offset value is 100, the value of HLEN(Header Length) is 5, and the value of the total length field is 100. What are the numbers of the first byte and last byte ?

Solution: The first byte number is 100 × 8 = 800. The total length is 100 bytes and the header length is 5 × 4 = 20 bytes, which means that there are 80 bytes in this datagram. If the first byte number is 800, the last byte number is 879.

5.3.5 IPv4 Limitations

Following are the major limitations of IPv4 addresses:

1. **Shortage of IP addresses:** IPv4 uses a 32 bit address, which generate 2^{32} (4 billion) possible addresses. Nowadays network is growing exponentially. Due to that IP addresses are getting tremendously consumed. So the unique addresses are becoming inadequate.
2. **Auto-configuration and mobility:** New technologies (mobile equipment, wireless network) are emerging and its use is quickly becoming common. There is no automatic way to automatically configure this kind of equipment in the network.
3. **Security:** The security option in IPv4 is optional, so it is not possible to keep all the data secure while it's routing through the network.
4. **Support for real time applications:** Services such as transmission of real time audio and video are becoming common nowadays. IPv4 does not provide ways for managing and reserving bandwidth for such real time transmissions.

5.4 IPV6 ADDRESSES

- Internet Protocol version 6 (IPv6) is the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet.
- IPv6 is an Internet Layer protocol for packet-switched internetworking and provides end-to-end datagram transmission across multiple IP networks, closely adhering to the design principles developed in the previous version of the protocol, Internet Protocol Version 4 (IPv4).

5.4.1 IPv6 Structure

- An IPv6 address consists of 16 bytes (octets); it is 128 bits long, (See Fig. 5.24).

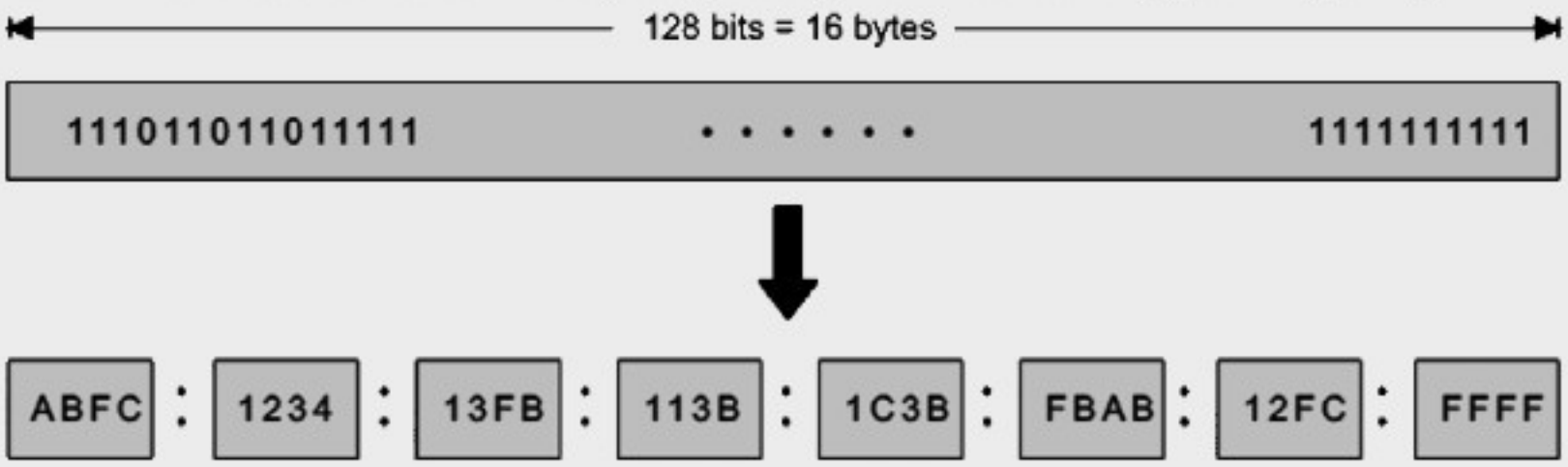


Fig. 5.24: IPv6 Address

Hexadecimal Colon Notation:

- To make addresses more readable, IPv6 specifies hexadecimal colon notation.
- In this notation, 128 bits are divided into eight sections, each of 2 bytes in length.
- Two bytes in hexadecimal notation require four hexadecimal digits.
- Therefore, the address consists of 32 hexadecimal digits, with every four digits separated by a colon.

Abbreviation:

- Although, IP addresses in hexadecimal format are very long, many of the digits are zeros, in this case we can abbreviate the address.
- The leading zeros of the section (four digits between two colons) can be omitted. Only leading zeros can be dropped, not the trailing zeros, (Refer Fig. 5.25).

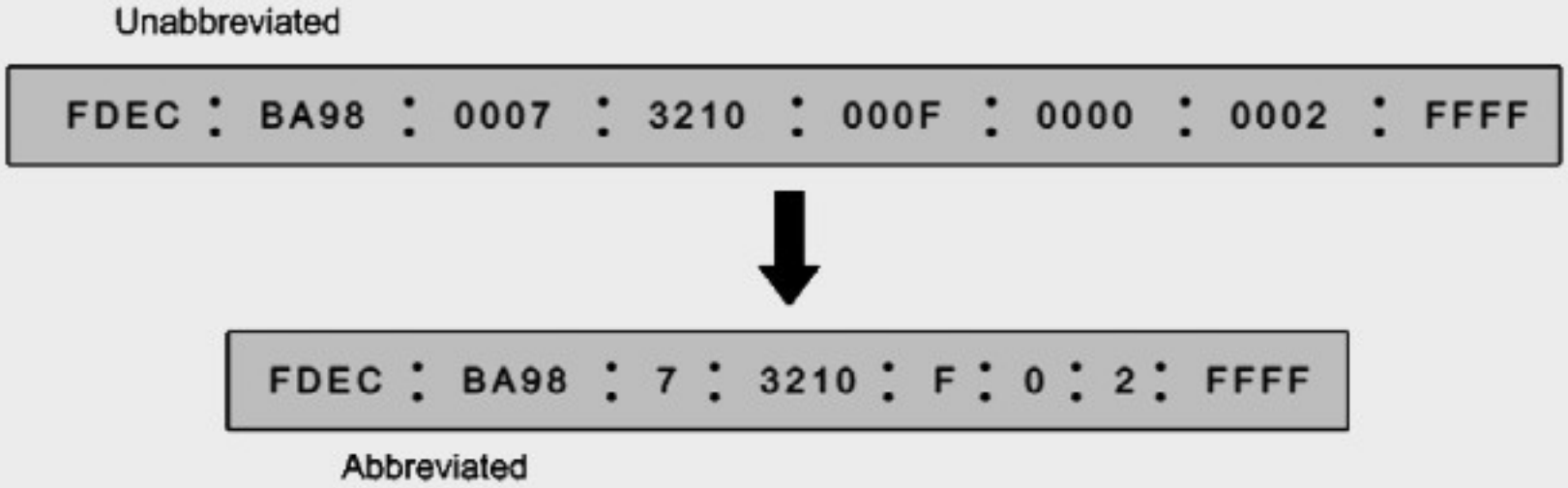


Fig. 5.25: Abbreviated Address

- Using this form of abbreviation, 0007 can be written as 7, 000F as F, and 0000 as 0. Note that 3210 can not be abbreviated.
- Further abbreviation is possible, if there are consecutive sections consisting of zeros only.
- We can remove the zeros altogether and replace them with double semicolon. Refer to the following figure. Note that this type of abbreviation is allowed only once per address. If there are two runs of zero sections, only one of them can be abbreviated.

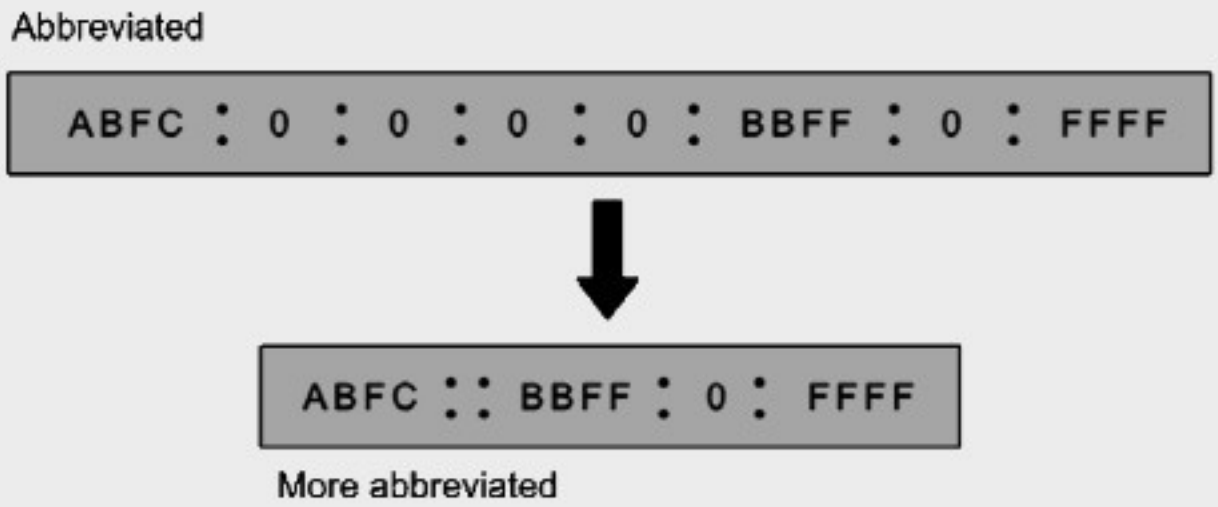


Fig. 5.26: Abbreviated Address with Consecutive Zeros

- Re-expansion of the abbreviated address is very simple: align the unabbreviated portions and insert zeros to get the original expanded address.

5.4.2 IPv6 Addresses Space (S-18)

- IPv6 addresses have 128 bits address space. The 128 bits of an IPv6 address are represented in 8 groups of 16 bits each. Each group is written as four hexadecimal digits and the groups are separated by colons (:).
- An example of this representation is 2001:0db8:0000:0000:0000:ff00:0042:8329.
- IPv6 defines three types of addresses:

1. **Unicast:**

- A unicast address defines a single computer. The packet sent to the unicast address must be delivered to that specific computer.

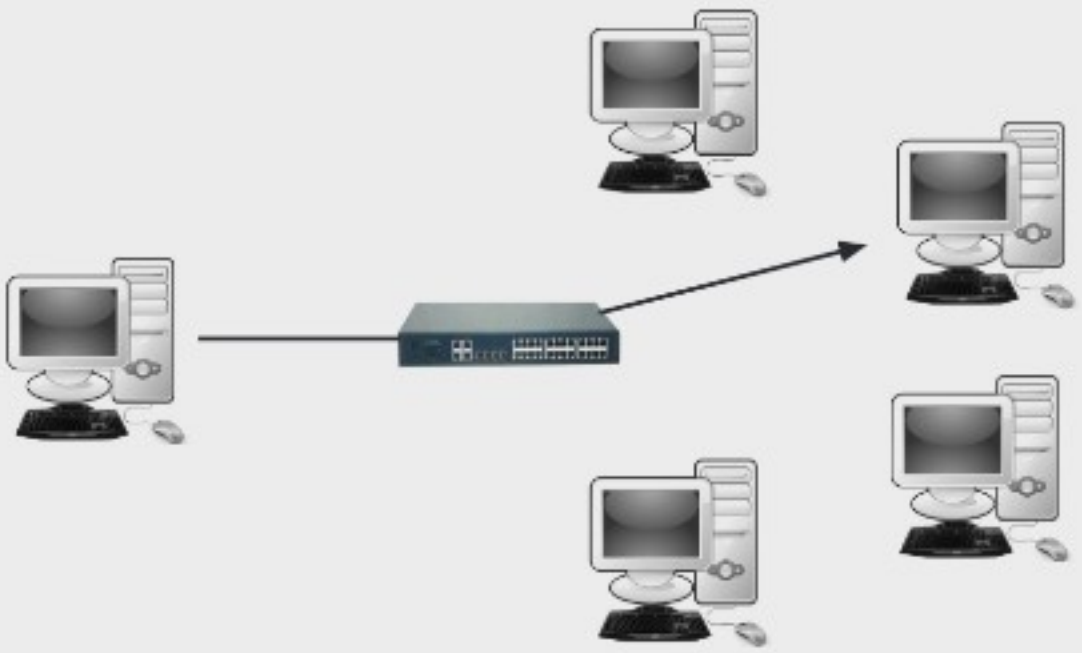


Fig. 5.27: Unicast Addressing

- IPv6 defines two types of unicast addresses: geographically based and provider based.
- A provider based address is generally used. The fields for provider based address are type identifier, registry identifier, provider identifier, subscriber identifier, subnet identifier, and node identifier.

2. Anycast:

- It defines a group of computers with addresses that have the same prefix. For example, all computers connected to the same physical network share the same prefix address.
- A packet sent to an anycast address must be delivered to exactly one of the members of the group – the closest or the most easily accessible.

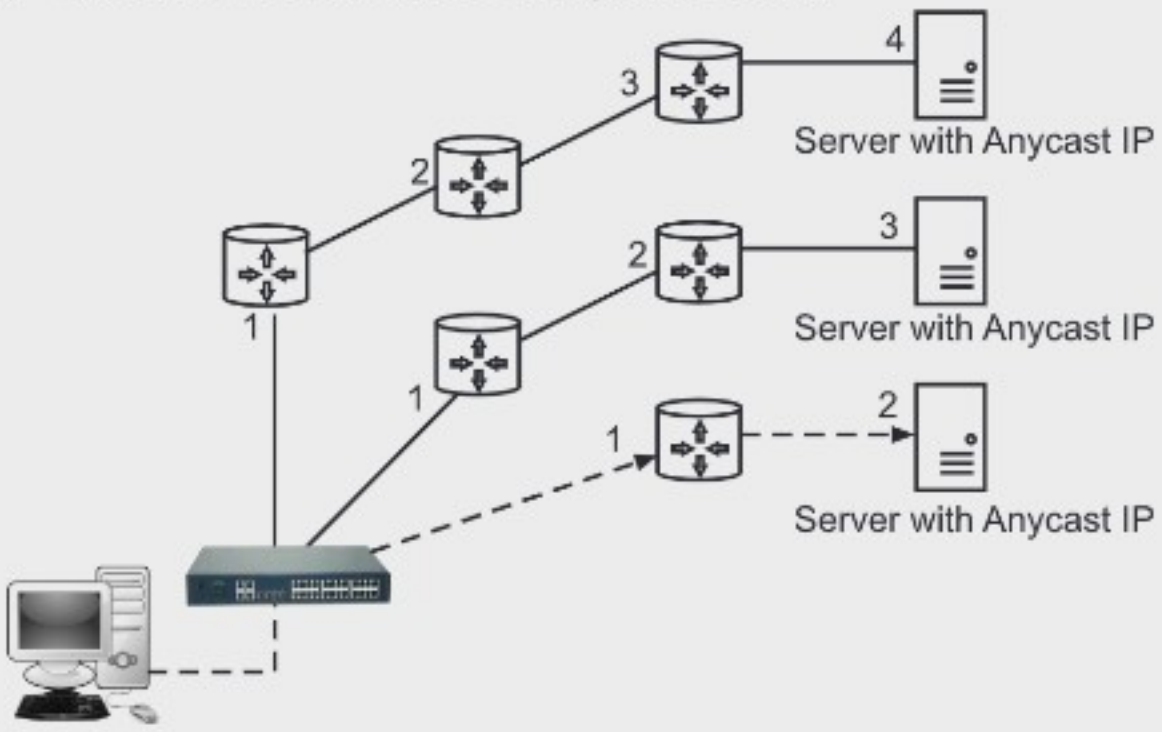


Fig. 5.28: Anycast Addressing

3. Multicast:

- It defines a group of computers. The packet sent to a multicast address must be delivered to each member of the group.

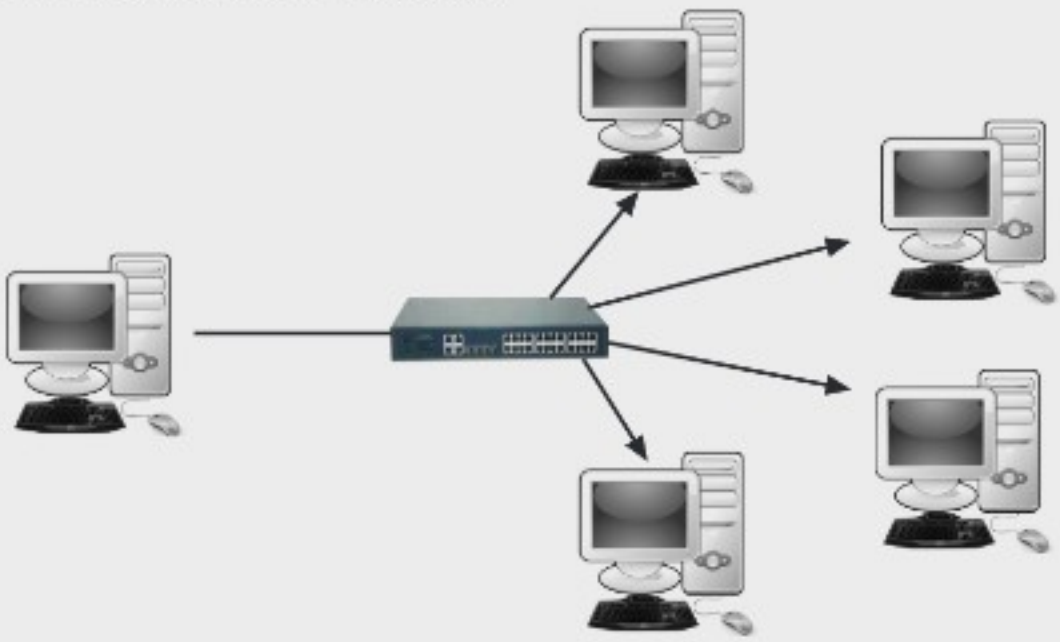


Fig. 5.29: Multicast Addressing

5.4.3 IPv6 Packet Format

- Fig. 5.30 shows the base header of IPv6 having fixed length of 40 octets, consisting of the following fields.

- Fields in IPv6 header are listed below:
  1. **Version:** Size is 4 bits. It specifies the internet protocol version number. For IPv6 it is 6.
  2. **Priority (Traffic class):** Size is 4 bits. It defines the priority of the packet with respect to traffic congestion.

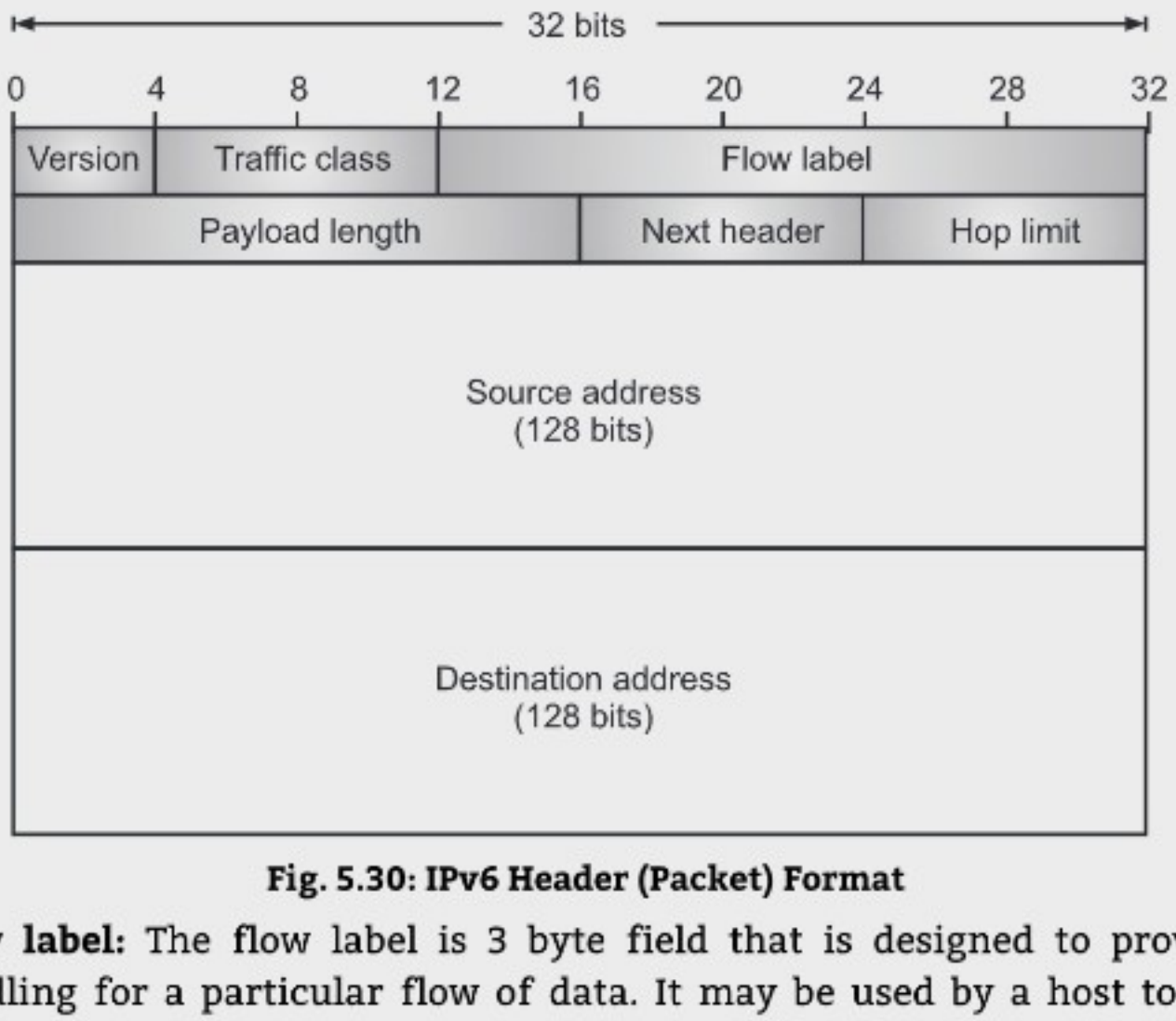


Fig. 5.30: IPv6 Header (Packet) Format

  3. **Flow label:** The flow label is 3 byte field that is designed to provide special handling for a particular flow of data. It may be used by a host to label those packets for which it is requesting special handling by routers within a network.
  4. Payload length: It is 16 bits field. It defines the total length of IP datagram including the base header.
  5. **Next header:** It is a 8 bits field. It identifies the type of header immediately following IPv6 header.
  6. **Hop Limit:** This is 8 bits field; it serves the same purpose as the TTL field in IPv4.
  7. **Source Address:** Source address is 128 bits field. It identifies the original source of the datagram.
  8. **Destination Address:** Destination address is a 128 bits field. It identifies the destination of the datagram.

5.4.4 Extension Header

- The length of the base header is fixed at 40 bytes. To get more functionality to the IP datagram, the base header can be followed by up to six extension headers.
- The Fig. 5.31 shows the types of extension headers.

- Various types of extension headers in Fig. 5.31 are explained below:
  1. **Hop-by-Hop Option:** It is used when sources need to pass the information to all routers visited by the datagram.
  2. **Source Routing:** It combines the concept of the strict source route and the loose source route option of the IPv4.

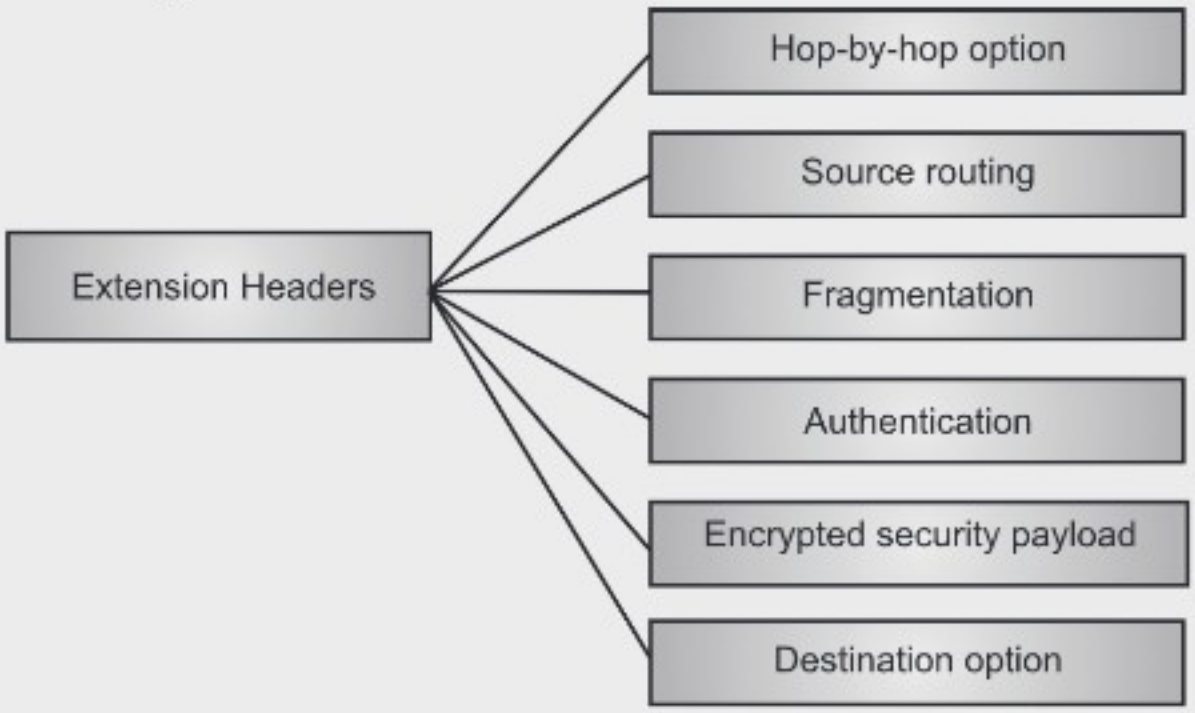


Fig. 5.31: Extension Header Types

  3. **Fragmentation:** In IPv4, the source or a router is required to fragment if the size of the datagram is larger than the MTU of the network over which the datagram travels. In IPv6, only the original source can fragment.
  4. **Authentication:** It validates the message sender and ensures the integrity of data.
  5. **Encrypted Security Payload (ESP):** It provides confidentiality and guards against eavesdropping.
  6. **Destination Option:** It is used when the source needs to pass information to the destination only. Intermediate routers are not permitted access to this information.

5.5 ADVANTAGES OF IPV6

- Due to the limitations of IPv4, IPv6 comes into existence. This is next-generation internet protocol and had many advantages on the previously existing version of Internet protocol (IPv4). These are listed below:

1. **Larger Address Space:**
   - An IPv6 address is 128 bits long (compared to IPv4, IPv6 address is very long because IPv4 address was only of 32 bits).
   - So total number of addresses generated using IPv6 is 2128.

2. **Better Header Format:**
   - IPv6 uses a new header format in which options are separated from the base header and inserted when needed, between base header and upper layer data.
   - This simplifies and speeds up the routing process because most of the options do not need to be checked by routers.
3. **New Options:**
   - IPv6 has new options to allow additional functionalities.
4. **Allowance for Extension:**
   - IPv6 is designed to allow the extension of the protocol if required by new technologies or applications.
5. **Support for Resource Allocation:**
   - In IPv6, the type of service field has been removed, but a mechanism (called flow label) has been added to enable the source to request special handling of packet.
   - This mechanism can be used to support traffic such as real time audio and video.
6. **Support for More Security:**
   - The encryption and authentication options in IPv6 provide confidentiality and integrity of the packet.
7. **Plug and Play:**
   - IPv6 includes plug and play in the standard specification. It therefore must be easier for beginner user to connect their machines to network, it will be done automatically.
8. **Clearer Specification:**
   - IPv6 follows good practices of IPv4, and rejects its minor problems.

5.6 IPV4 VS IPV6

- Following table shows the difference between IPV4 and IPV6.

Table 5.7: Difference between IPv4 And IPv6:

Sr. No.	IPv4	IPv6
1.	It is 32 bit source and destination addresses	It is 128 bit source and destination addresses.
2.	There are a maximum of 232 IP addresses.	There are maximum 2128 IP addresses.
3.	IPv4 addresses are written by dotted decimal notation. For example: 10.15.11.23.	IPv6 addresses are written in hexadecimal colon notation. For example: FADB:A2B2:A453:1212:AAB3:ADBD:BBCC:1234

Contd...

4.	Basic length of IPv4 header is 20 bytes (excluding option field).	Length of IPv6 header is 40 bytes.
5.	IPv4 header has a checksum.	It has no header checksum.
6.	Security is an optional parameter.	It has been designed to satisfy the growing and expanded need for network security.
7.	Headers include option fields.	No option field is present in the basic header. All optional data is moved to the extension header.
8.	IPsec support is optional.	IPsec support is compulsory.
9.	Manual or DHCP configuration is required.	Gets automatically configured, no need of manual and DHCP configuration.

Summary

- In the seven layer OSI model of computer networking, the network layer is layer 3rd. Network layer receives services from the data link layer and gives services to the transport layer.
- The network layer is responsible for the delivery of individual packets from the source to the destination host. This layer is also responsible for routing mechanism, addressing, internetworking, packetizing and fragmentation etc.
- The network design issues of network layer includes Store-and-Forward Packet Switching, the services provided to the transport layer, Internal design of the subnet, Routing, Congestion control, and Internetworking etc.
- Store and forward is a communication technique in which information is sent to an intermediate station where it is kept and sent at a later time to the final destination or to another intermediate station.
- For connection-oriented service, we need a virtual-circuit subnet. The idea behind virtual circuits is to avoid having to choose a new route for every packet sent. If connectionless service is offered, packets are injected into the subnet individually and routed independently of each other. No advance setup is needed.
- The packets transmitted by the source computer may pass through several LANs or WANs before reaching at the destination computer. To identify every device uniquely on the Internet, we need a global addressing scheme, called logical addressing.
- A logical address is given to all hosts connected to the Internet and this logical address is called Internet Protocol (IP) Address.
- An IPv4 (Internet Protocol version 4) address is a 32-bit address that uniquely and universally defines the connection of a device such as a computer or a router to the Internet.
- IPv4 addressing uses the concept of classes. This architecture is called classful addressing.

- To overcome address depletion and give more organizations access to Internet, classless addressing was designed and implemented. No classes are used but the addresses are still granted in blocks.
- A better way to define block of addresses is to select any address in the block and the mask. The mask is 32 bit number in which the n left most bits are 1s and the 32-n rightmost bits are 0s.
- When classful addressing was used, subnetting was introduced. If an organization was granted a large block in class A or B, it could divide the addresses into several contiguous groups and assign each group to smaller networks (subnets).
- Subnetting is the process of dividing a network into smaller networks called subnets or sub networks. Each of these subnets has its own specific address.
- In supernetting, an organization can combine several class C blocks to create a larger range of addresses. In other words, several networks are combined to create a supernetwork or a supernet.
- Supernetting is an addressing scheme in which several class C blocks can be combined to create a larger range of addresses.
- Network Address Translation (NAT) is a methodology of remapping one IP address space into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device.
- A translation table has only two columns i.e., the private address and the external address (destination address for a packet).
- IPv4 is defined and specified in IETF publication RCF 791.
- A datagram can be defined as, "a self-contained, independent entity of data carrying sufficient information to be routed from the source to the destination computer without reliance on earlier exchanges between this source and destination computer and the transporting network."
- In IPv4, packets are called as datagrams or headers.
- The Internet Protocol (IP) implements datagram fragmentation, breaking it into smaller pieces, so that packets may be formed that can pass through a link with a smaller Maximum Transmission Unit (MTU) than the original datagram size.
- To compute checksum in IPv4, the value of the checksum field is set to 0. Then the entire header is divided into 16 bit sections and added together. The result (sum) is complemented and inserted into the checksum field. The checksum covers only the header, not the data.
- The header of IPv4 datagram is of two parts: Fixed part and Variable part. The fixed part is of 20 bytes long and variable part is maximum of 40 bytes. Options are not required for a datagram, they are used for network testing and debugging.
- An IPv6 address consists of 16 bytes (octets); it is 128 bits long.
- IPv6 defines three types of addresses: Unicast, Anycast, Multicast.
- The base header of IPv6 has a fixed length of 40 octets.
- The length of the base header is fixed at 40 bytes. To get more functionality to the IP datagram, the base header can be followed by up to six extension headers.
- The extension headers are Hop-by-Hop option, Source Routing, Fragmentation, Authentication, Encrypted security Payload (ESP), Destination Option.

Check Your Understanding

1. The ability of a single network to span multiple physical networks is known as _____
   (a) Subnetting (b) Masking
   (c) Fragmenting (d) Hopping
2. The network layer is concerned with _____ of data.
   (a) bits (b) frames
   (c) packets (d) bytes
3. A 4 byte IP address consists of _____
   (a) only network address
   (b) only host address
   (c) network address & host address
   (d) network address & MAC address
4. Which one of the following is not a function of network layer?
   (a) routing (b) inter-networking
   (c) congestion control (d) error control

ANSWER KEY

1. (a)	2. (c)	3. (c)	4. (d)	

Practice Questions

Q.1: Answers the Following Questions in short.

1. List the network layer services.
2. Define internetworking and routing.
3. What is multicasting?
4. How to find classes of IP address in binary and dotted decimal notations ?
5. What is logical address?
6. What is classful addressing?
7. Why time to live field is required in IP datagram.
8. What is a use of timestamp option?
9. State any two goals in the designing of network layer services.
10. List out various types of extension headers.

Q.2: Answers the Following Questions:

1. State the advantages of network layer.
2. State differences between IPv4 and IPv6.
3. State the advantages of IPv6 over IPv4.
4. Explain the task performed by network layer.
5. What is the need of network address translation? How does NAT router maintain translation table?
6. Explain IPv4 fragmentation process in detail.

7. The value of the total length field in an IPv4 datagram is 36 and the value of the header length field is 5. How many bytes of data is the packet carrying?
8. Why network address translation is needed? How it is implemented?
9. Write note on the extension header of IP datagram.
10. Find out class, Netid and Hostid of: IP address 126.25.21.1.
11. Draw the structure of IPv4 datagram and explain its fields.

Q.3: Questions on Problems:

1. Change the following IP addresses from binary notation to dotted decimal notation:
   (a) 01111111 11110000 01100111 11111001
   (b) 10101111 11000111 11111000 00011101
   (c) 11011111 10110000 00011111 01011101
   (d) 11100000 11110111 1100011 01111101.
2. Find the class, netid and host id of the IP address:
   (a) 114.34.12.8 (b) 127.24.6.10
   (c) 240.34.54.15 (d) 230.34.2.1
   (e) 237.14.2.10 (f) 129.14.6.8.
3. Change the IP addresses given in question 2 from dotted decimal to binary notation.
4. An ISP is granted a block of addresses starting with 140.80.0.0/16. The ISP wants to distribute these blocks to 2600 customers as follows:
   (a) The first group has 200 medium size businesses, each needs 16 addresses.
   (b) The second group has 400 small businesses, each needs 8 addresses.
   (c) The third group has 2000 households, each needs 4 addresses.
   (d) Design the sub-blocks and give the slash notation for each sub-block. Find out how many addresses are still available after these allocations.
5. Find the range of addresses in the following blocks:
   (a) 200.17.21.128/27 (b) 200.17.21.128/25
   (c) 17.34.16.0/23 (d) 123.56.77.32/29
6. An organization is granted the block 211.17.180.0/24. The administrator wants to create 32 subnets:
   (a) Find the subnet mask.
   (b) Find the number of addresses in each subnet.
   (c) Find the first and last addresses in subnet 1.
   (d) Find the first and last addresses in subnet 32.
7. A host is sending 100 datagrams to another host. If the identification number of the first datagram is 1024. What is the identification number of the last?
8. The value of the total length field in an IPv4 datagram is 36 and the value of the header length field is 5. How many bytes of data is the packet carrying?

Q.4: Define following terms.

(a) Netid (b) Hostid
(c) Classless addressing (d) Subnetting
(e) Supernetting

Previous Exam Questions

Summer 2019

1. What is Checksum ? **[1 M]**

Ans. Refer to section 5.3.3

3. Explain supernetting. **[4 M]**

Ans. Refer to section 5.2.6

4. Explain the fields in IPV4 datagram. **[4 M]**

Ans. Refer to section 5.3.1

Winter 2018

1. Define internetworking and routing. **[1 M]**

Ans. Refer to section 5.1

2. Define Netid and Hostid. **[3 M]**

Ans. Refer to section 5.2.2

3. Explain network address translation in brief. **[4 M]**

Ans. Refer to section 5.2.4

4. Explain subnetting and supernetting. **[5 M]**

Ans. Refer to section 5.2.5, 5.2.6

Summer 2018

1. The length of IP address is_____ bits. **[1 M]**

(i) 46 **(ii) 32**

(iii) 16 (iv) 64

2. Convert following IPV4 address from decimal rotation to binary: **[1 M]**

221.34.7.82

Ans. Refer to Example 2

3. Define netid and hostid. **[1 M]**

Ans. Refer to section 5.2.2

4. Explain IPV6 address space. **[3 M]**

Ans. Refer to section 5.4.2

5. Explain supernetting. **[4 M]**

Ans. Refer to section 5.2.6

6. Explain the fields in IPV4 datagram. **[3 M]**

Ans. Refer to section 5.3.1

❖❖❖

6...

Transport and Application Layer

Objectives...

- To understand the Transport Layer.
- To study UDP and TCP Protocols.
- To study Process-to-Process Delivery, Multiplexing and Demultiplexing.
- To understand TCP vs UDP.
- To learn about Domain Name System.

6.1 INTRODUCTION

- Transport layer is number four (4) in the OSI model is responsible for process-to-process delivery. To achieve the process-to-process delivery, the transport layer supports three protocols i.e., UDP (User Datagram Protocol), TCP (Transmission Control Protocol), SCTP (Stream Control Transmission Protocol).
- The application layer provides full end-user access to a variety of shared network services for efficient OSI model data flow. This layer has many responsibilities, including error handling and recovery, data flow over a network and full network flow. It is also used to develop network-based applications.
- In this chapter we discussed two protocols UDP and TCP in detail.

6.2 PROCESS-TO-PROCESS DELIVERY

- We know that the data link layer is responsible for delivery of frames between two neighboring nodes over a link. This is called node-to-node delivery.
- The network layer is responsible for delivery of datagram between two hosts. This is called host-to-host delivery.
- Real communication takes place between two processes (application programs) in a network. This is called process-to process delivery.

- The transport layer is responsible for process-to-process delivery, the delivery of a packet, part of a message, from one process to another.
- At the transport layer, we need a transport layer address, called a port number, to choose among multiple processes running on the destination host.
- In the Internet model, the port numbers are 16-bit integers between 0 and 65,531.
- The client program defines itself with a port number, chosen randomly by the transport layer software running on the client host. This is the ephemeral port number.
- The server process must also define itself with a port number. This port number, however, cannot be chosen randomly.
- On source and destination, several processes are running simultaneously. To complete the delivery, a mechanism is required to deliver data from one of these processes running on the source host to the corresponding destination host.
- Fig. 6.1 shows these three types of deliveries.

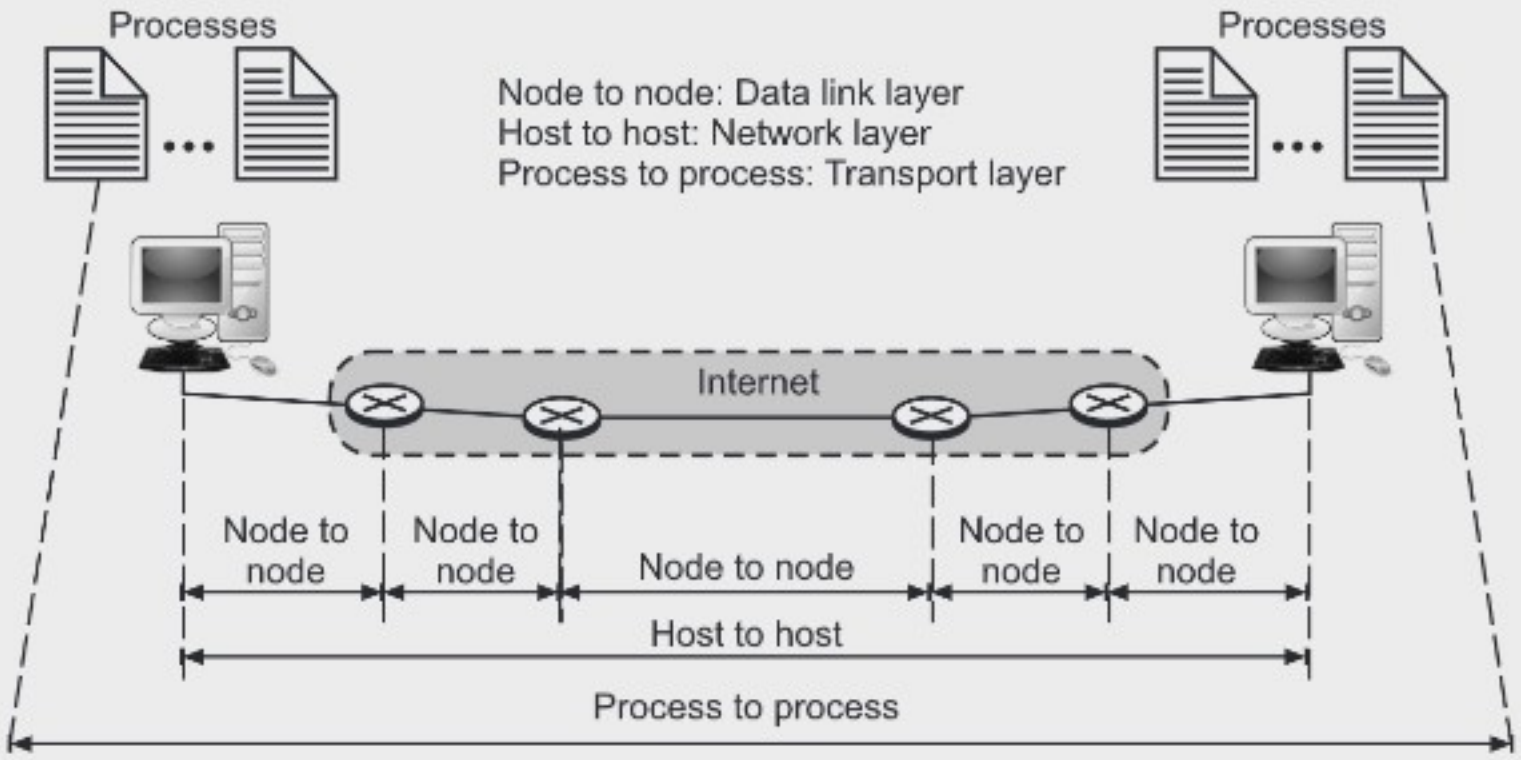


Fig. 6.1: Three Types of Deliveries

6.2.1 Multiplexing and Demultiplexing

- Multiplexing and Demultiplexing are the two very important functions that are performed by a transport Layer.

Multiplexing:

- Transport layer at the sender side receives data from different applications, but there is only one transport protocol, which encapsulates every packet with a Transport Layer header and passes it on to the underlying Network Layer. This is a many-to-one relationship. This job of transport layer is known as Multiplexing.

Demultiplexing:

- At receiver, the situation is opposite, the relationship is one-to-many and requires demultiplexing.
- Transport layer receives packets from the network layer. After removing the header, the transport layer delivers each message to the appropriate process as per port number.

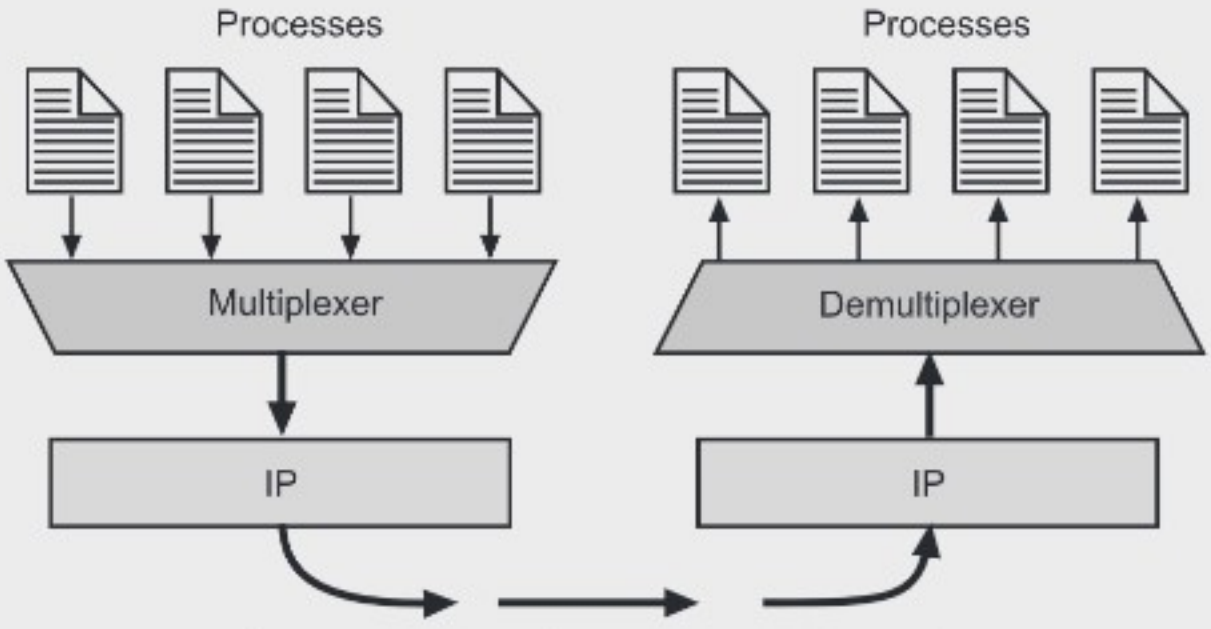


Fig. 6.2: Multiplexing and Demultiplexing

6.3 USER DATAGRAM PROTOCOL (UDP)

- The UDP is one of the core members of the Internet protocol suite. The protocol was designed by David P. Reed in 1980 and formally defined in RFC 768 standard.
- UDP is a connectionless, unreliable Transport Layer protocol.
- UDP does not add anything to the services of IP except to provide process-to-process communication instead of host-to-host communication. Also, it performs very limited error checking.
- UDP is a very simple protocol, using minimum overhead. If a process wants to send a small message and does not care much about reliability, it can use UDP.
- UDP is stateless protocol. It is a suitable protocol for streaming applications such as VoIP, multimedia streaming.

6.3.1 Datagram Format

- UDP packets are called as user datagrams, have a fixed-size header of 8 bytes.
- Fig. 6.3 shows the format of a User Datagram Protocol.
- UDP header contains four main parameters:

1. **Source Port Number:** This 16 bit field is used by the process running on the source host which wants to make communication. Port number can range from 0 to 65,531. If a client is sending a request, generally the port number is an ephemeral port number. If the server is sending a response the port number is well known port number.

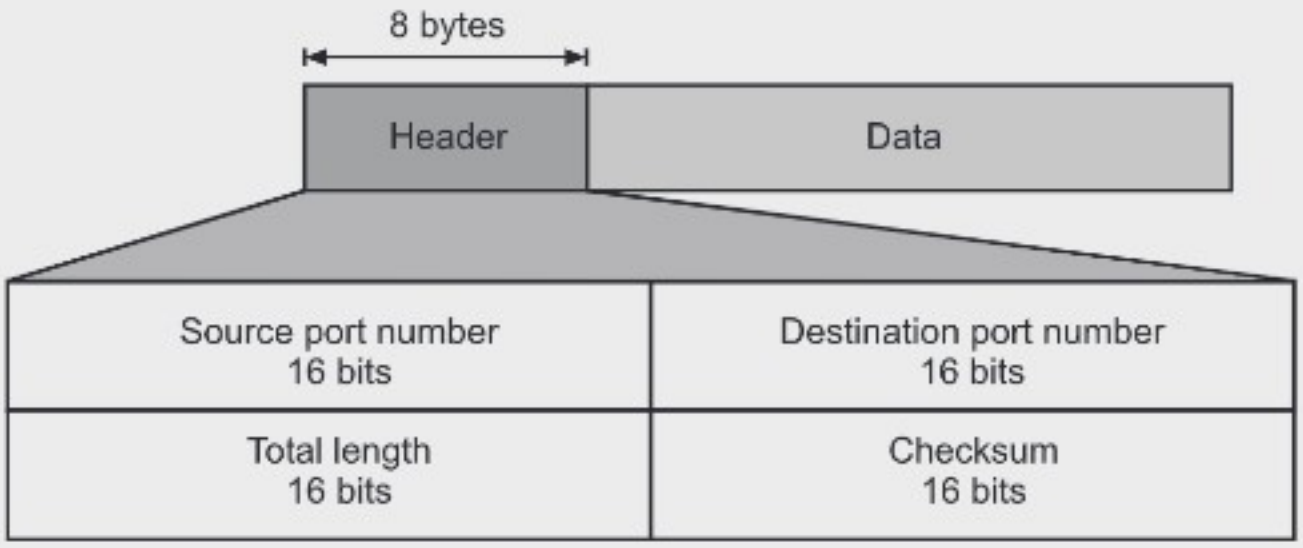


Fig. 6.3: Datagram Format of UDP

2. **Destination Port:** This 16 bit is used by the process running on the destination host. If the destination host is a server, the port number is a well known port number. If the destination host is a client, the port number is an ephemeral port number.
3. **Length:** This 16 bit field defines the total length of the user datagram, header plus data. This field is actually not necessary, because UDP is encapsulated in IP. IP has total length and header length fields.

   So, UDP length = IP length – IP header's length
4. **Checksum:** This 16 bit field is used to detect errors over the entire user datagram. The checksum field we will discuss in detail in this chapter.

- Some well known ports used by UDP are given in Table 6.1.

Table 6.1: Some well known ports used by UDP

Port	Protocol	Description
7	Echo	Echoes a received datagram back to the sender.
9	Discard	Discards any datagram that is received.
11	Users	Active users.
13	Day time	Returns the date and time.
17	Quote	Returns a quote of the day.
53	Name server	Domain name service.
67	BOOTPs	This is the server port to download the bootstrap information.
68	BOOTPc	This is the client port to download bootstrap information.
69	TFTP	Trivial File Transfer Protocol.
111	RPC	Remote Procedure Call.
123	NTP	Network Time Protocol.
161	SNMP	Simple Network Management Protocol.

6.3.2 Checksum

- UDP provides checksums for data integrity, and port numbers for addressing different functions at the source and destination of the datagram.
- The UDP checksum calculation is different from IP. UDP's checksum includes three sections namely a pseudo header, the UDP header and the data coming from the application layer.
- The pseudo header is the part of the header of the IP packet in which the user datagram is to be encapsulated with some fields filled with 0s.

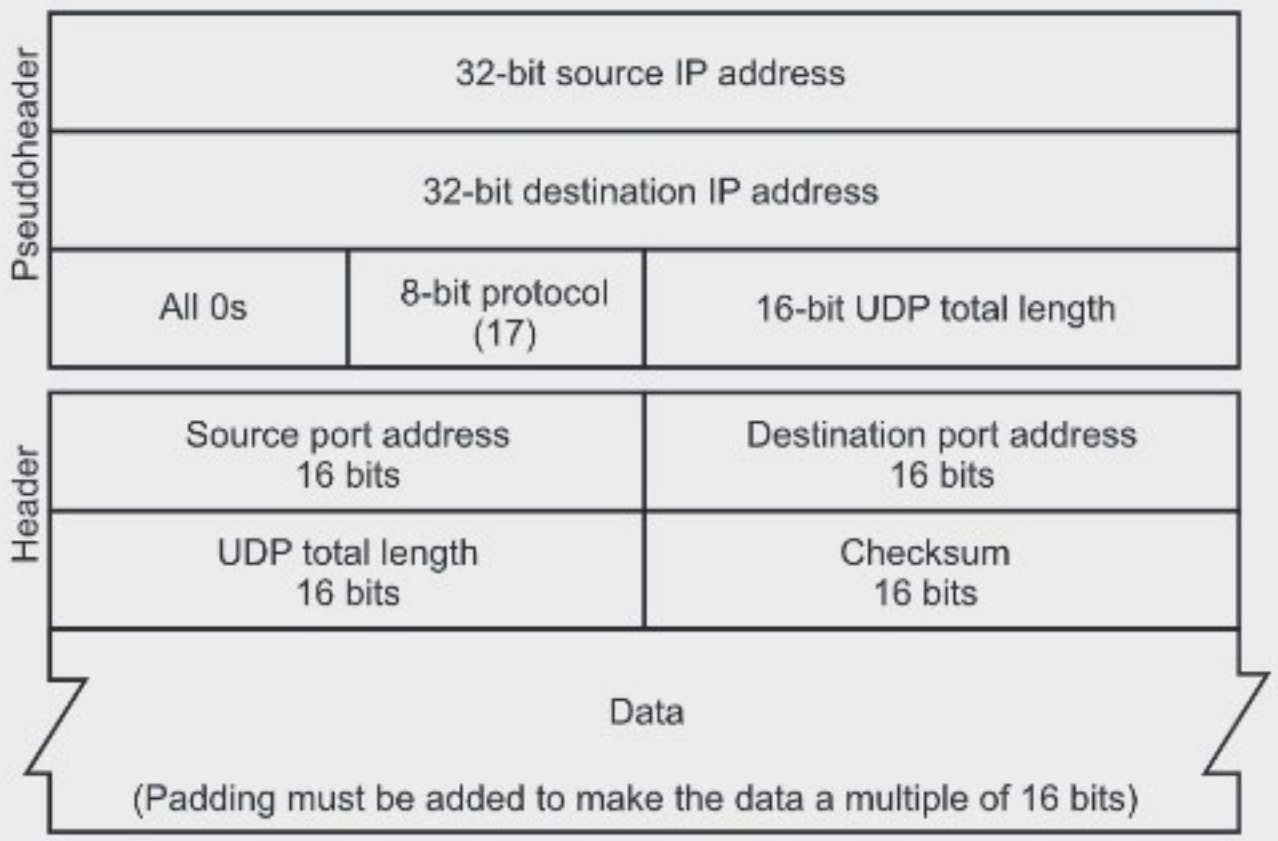


Fig. 6.4: Pseudoheader for Checksum Calculation

- If the checksum does not include the pseudo header, a user datagram may arrive safe and sound. If the IP header is corrupted, it may be delivered to the wrong host.
- The protocol field is added to confirm that the packet belongs to UDP. The value of protocol for UDP is 17. If this value is changed during transmission, the checksum calculation at the receiver will detect it and UDP drops the packet.
- The calculation of checksum and its inclusion in a user datagram are optional. If checksum is not calculated, the field is filled with 1s.

  Example: Fig. 6.5 shows the checksum calculation for a very small user datagram with only 7 bytes of data. Since the data is odd, padding is added for checksum calculation. The pseudo header as well as the padding will be dropped when the user datagram is delivered to IP.

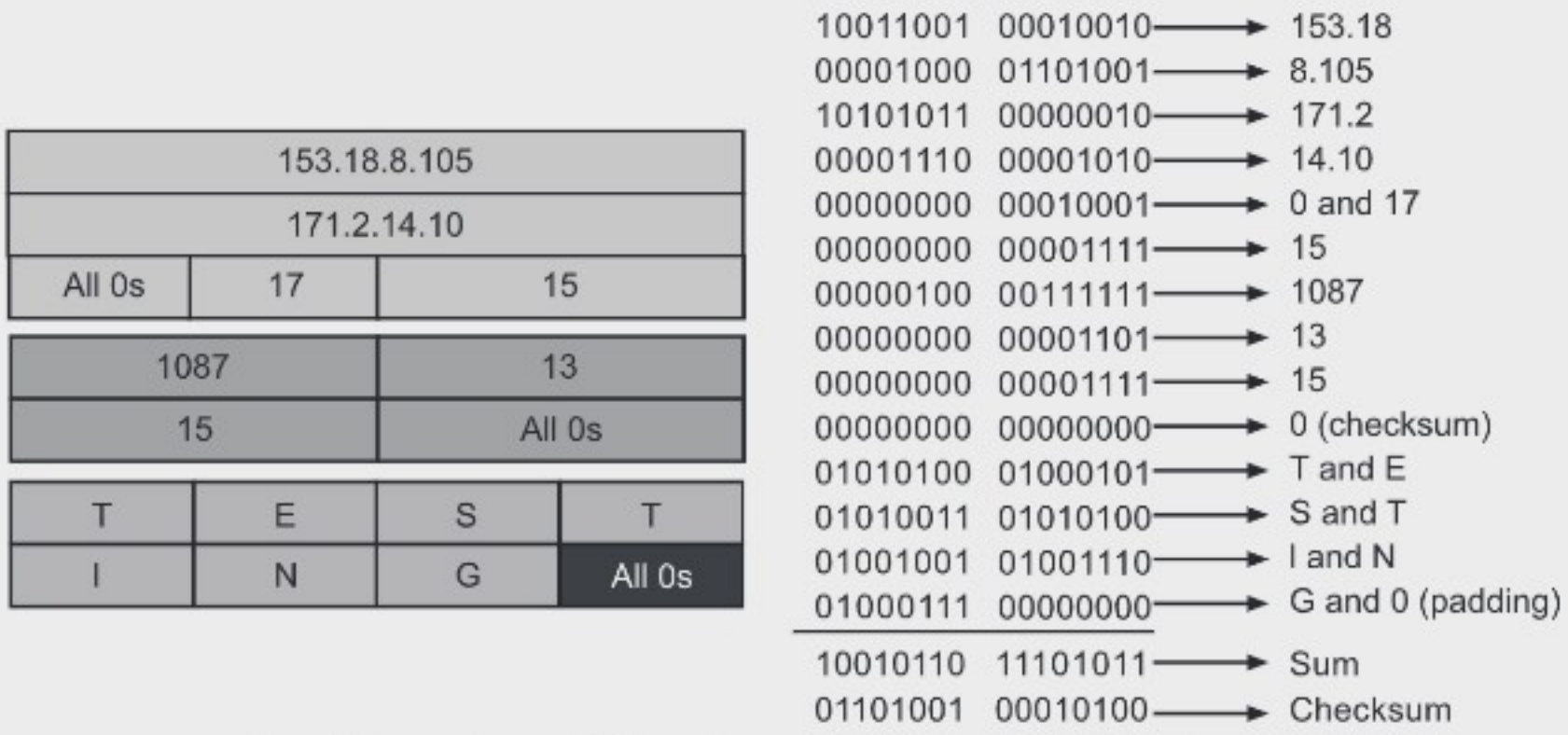


Fig. 6.5: Checksum Calculation of a Simple UDP User Datagram

6.3.3 UDP Operations

- UDP uses concepts common to the transport layer. These concepts are explained below:

1. Connectionless Services:

UDP provides connectionless service. The user datagram is not numbered. There is no connection establishment and no connection termination between both ends. Every user datagram is an independent datagram, they can travel on a different path.

The process that uses UDP cannot send a stream of data to UDP, instead each request must be small enough to fit into one user datagram. Only those processes sending short messages should use UDP.

2. Flow and Error Control:

UDP is a simple, unreliable transport protocol, which does not provide error and flow control.

Since, there is no flow control, the receiver may overflow with incoming messages. Since, there is no error control, the sender does not know if a message has been lost or duplicated.

Absence of flow and error control means that the process using UDP should provide these mechanisms.

3. Encapsulation and Decapsulation:

To send a message from one process to another, the UDP protocol encapsulates and decapsulates messages in an IP datagram.

4. Queuing:

- In UDP, queues are associated with ports as shown in Fig. 6.6.
- At the client site, when a process starts, it requests a port number from the Operating System (OS).
- An incoming and an outgoing queue associated with each process is created.

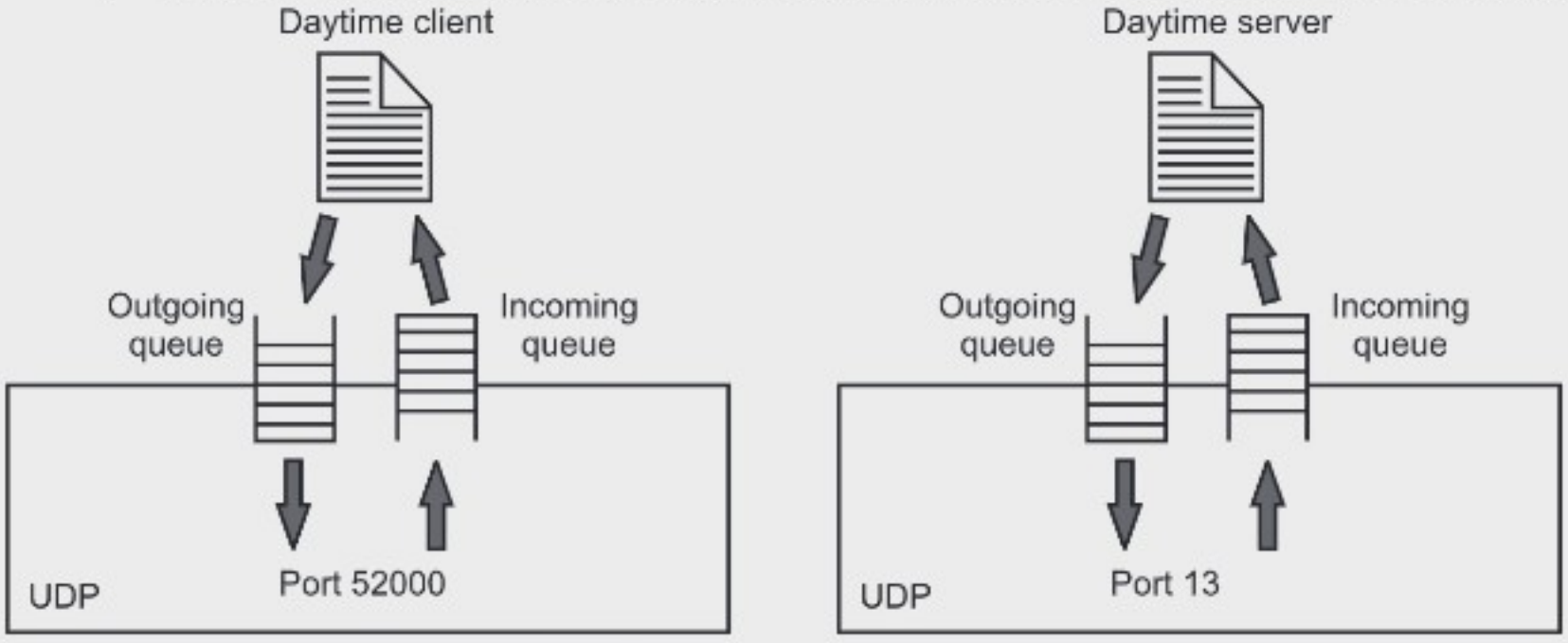


Fig. 6.6: Queuing in UDP Operations

- Even if a process wants to communicate with multiple processes, it obtains only one port number and one outgoing and one incoming queue. Queues work as long as the process is running, when the process terminates, the queues are destroyed.
- The client process can send messages to the outgoing queue by using the source port number. UDP removes the messages one by one and after adding the UDP header, delivers it to IP. If the outgoing queue is overflow, the operating system asks the client process to wait before sending any messages.
- When a message arrives for a client, UDP checks the destination port number and a queue which is created for such port. If there is such a queue, UDP sends the received user datagram to the end of the queue. If such queue is not created, UDP discards such datagram. An incoming queue can overflow, if this happens, UDP drops the user datagram.
- At the server site, the mechanism for creating queues is different. When server starts running, incoming and outgoing queues are created. When message arrives for a server, UDP checks for port number, if there is a queue created for port number UDP sends the received datagram to the end of the queue. If there is no such queue, UDP discards the user datagram. If the incoming queue is overflowed, UDP drops the packets.
- When server wants to send a message to the client, it sends a message to the outgoing queue by using the source port number specified in the request. UDP removes messages one by one, adds UDP header and delivers them to IP. If an outgoing queue is overflow, the operating system asks the server to wait before sending more messages.

6.3.4 Use of UDP

- Following are the uses of UDP :
  1. UDP is suitable for a process that requires simple request response communication with little concern for flow control and error control.
  2. UDP is suitable for a process having inbuilt error control and flow control mechanisms, for example, TFTP (Trivial File Transfer Protocol).
  3. UDP is used for route updating protocols such as RIP (Routing Information Protocol).
  4. UDP is suitable for multicasting .
  5. UDP is used for management processes such as SNMP (Simple Network Management Protocol).

6.4 TRANSMISSION CONTROL PROTOCOL (TCP)

- The TCP is one of the most important protocols of the Internet Protocols suite. TCP is the most widely used protocol for data transmission in communication network such as Internet.
- TCP is a reliable and connection oriented protocol.
- TCP creates a virtual connection between two TCPs to send data. The receiver always sends either positive or negative acknowledgement about the data packet to the sender, so that the sender always has the right clue about whether the data packet has reached the destination or it needs to resend it.
- In addition, TCP uses flow and error control mechanisms. All these features make TCP a reliable protocol.

6.4.1 TCP Services

- Let us discuss the services offered by TCP to the process at the application layer.

1. Process-to-process Communication:

- Like UDP, TCP provides process-to-process communication using port numbers.
- Table 1.2 shows some well-known port numbers used by TCP.

Table 6.2: Well known ports used by TCP

Port	Protocol	Description
7	Echo	Echoes a received datagram back to the sender.
9	Discard	Discards any datagram that is received.
11	Users	Active users.
13	Day time	Returns the date and time.
17	Quote	Returns a quote of the day.

Port	Protocol	Description
19	Chargen	Returns a string of characters.
20	FTP, Data	File Transfer Protocol (data connection).
21	FTP, Control	File Transfer Protocol (control connection).
23	TELNET	Terminal Network.
25	SMTP	Simple Mail Transfer Protocol.
53	DNS	Domain Name Server.
67	BOOTP	Bootstrap Protocol.
80	HTTP	Hypertext Transfer Protocol.
111	RPC	Remote Procedure Call.

2. Stream Delivery Service:

- TCP is a stream oriented protocol. TCP allows the sending process to deliver data as a stream of bytes and allows the receiving process to obtain data as a stream of bytes.
- TCP creates an environment in which the two processes seem to be connected by an imaginary "tube". This tube carries data across the Internet. This imaginary environment is shown in Fig. 6.7.
- The sending process produces the stream of bytes and the receiving process reads data from it.

Fig. 6.7: Stream Delivery

3. Sending and Receiving Buffers:

- TCP requires buffers for data storage, since the sending and receiving processes may not write or read data at the same speed.
- There are two buffers, sending buffer and receiving buffer.
- Fig. 6.8 shows the movement of the data in one direction. At the sending side, the buffer is divided into three sections. The white section is empty, that can be filled by the sending process.

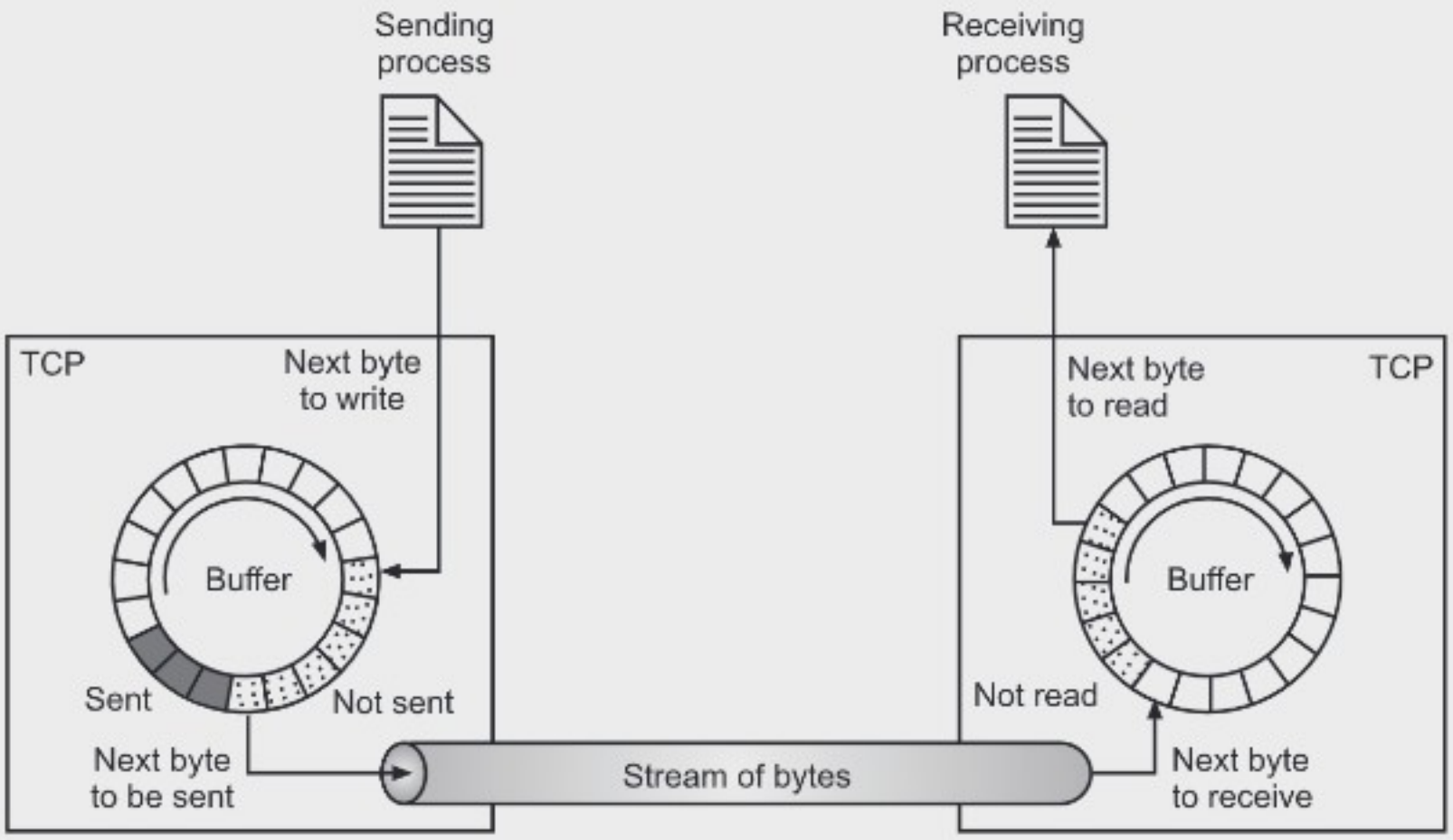


Fig. 6.8: Sending and Receiving Buffers

- At the sending site, the buffer has three sorts of chambers. The white section contains empty chambers which will be filled by the sending process (producer). The grey area holds bytes that are sent but not yet acknowledged. TCP keeps these bytes within the buffer until it receives an acknowledgment. The dotted area contains bytes to be sent by the sending TCP.
- At the receiving site, the operation of the buffer at the receiver site is easier . The circular buffer is split into two areas (shown as white and dotted). The white area contains empty chambers to be filled by bytes received from the network. The dotted sections contain received bytes which will be read by the receiving process. When a byte is read by the receiving process, the chamber is recycled and added to the pool of empty chambers.

4. Segments:

- Fig. 6.9 shows segments in TCP.
- IP provides services to TCP. IP protocol needs to send data in packets, not as a stream of bytes. At the transport layer, TCP groups a number of bytes together into packets called a segment.
- TCP adds a header to each segment and delivers it to IP, for transmission. The segments are encapsulated in IP datagram and transmitted.

5. Full Duplex Communication:

- TCP offers full duplex communication in which data can flow in both directions at the same time.

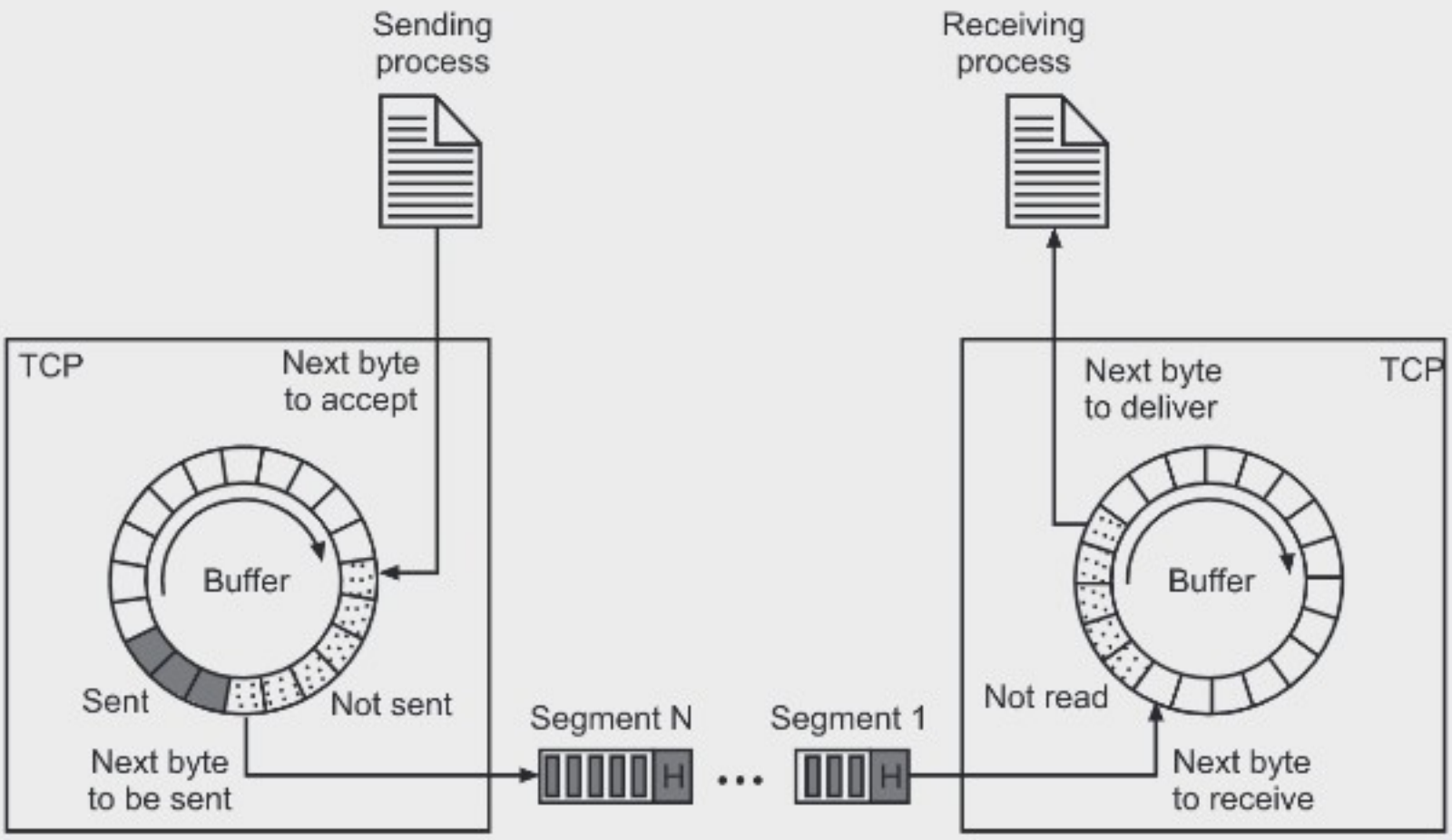


Fig. 6.9: TCP Segments

6. **Connection Oriented Service:**

- TCP is a connection oriented protocol. When a process at site A wants to send and receive data from another process at site B, the following occurs:
  (i) The two TCPs establish a connection between them.
  (ii) Data is exchanged in both directions.
  (iii) The connection is terminated.

7. **Reliable Service:**

- TCP is connection oriented and reliable protocol. It uses acknowledgement to check the arrival of data.

6.5 TCP FEATURES

- To provide the services mentioned above, TCP has several features that are explained below:

1. **Numbering System:**

- TCP software keeps track of segment (packets) transmitted and received. But there is no number value in the segment header.
- There are two fields i.e., sequence number and the acknowledgement number. These two fields refer to the byte number and not the segment number.

2. **Byte Number:**

- TCP numbers all data bytes that are transmitted in a connection.
- Numbering is independent in each direction. The numbering starts with a randomly generated number.

3. **Sequence Number:**

- The value in the sequence number field of a segment defines the number of the first byte contained in that segment. When a segment carries a combination of data and control information (piggybacking), it uses a sequence number.
- If a segment does not carry user data, it does not logically define a sequence number. The field is there but value is not valid. Randomly generated sequence numbers are used. If it is x then the first byte sequence number is x+1.

4. **Acknowledgement Number:**

- Communication in TCP is full duplex. Both communication parties send and receive data at the same time.
- Every party starts with a different sequence number. Each party also uses an acknowledgment number to confirm the bytes it has received.
- The value of the acknowledgement field in a segment defines the number of the next byte a party expects to receive. The acknowledgement number is cumulative.

5. **Flow Control:**

- TCP provides a flow control mechanism. The receiver of data controls the amount of data that are to be sent by the sender. By doing this, the receiver is not swamped by data sent by the sender.
- The numbering system allows TCP to use a byte oriented flow control.

6. **Error Control:**

- For providing reliable service, TCP uses error control mechanisms. Error control is byte oriented.

7. **Congestion Control:**

- TCP also provides congestion control. Receiver not only controls the amount of data sent by the sender (flow control), but it is also determined by the level of congestion in the network.

6.6 TCP SEGMENT FORMAT

- A packet in TCP is called segment. The format of TCP packet is shown in Fig. 6.10.
- The segment consists of 20 to 60 bytes header, followed by data from the application layer. The header is of 20 bytes if no options are used and upto 60 bytes if it contains options.
- Fig. 6.10 shows following fields of TCP segment format:
  1. **Source Port address:** This 16 bit field defines the port number of the application program in the host that is sending the segment.
  2. **Destination Port address:** This 16 bit field defines the port number of the application program in the host who is receiving the segment.

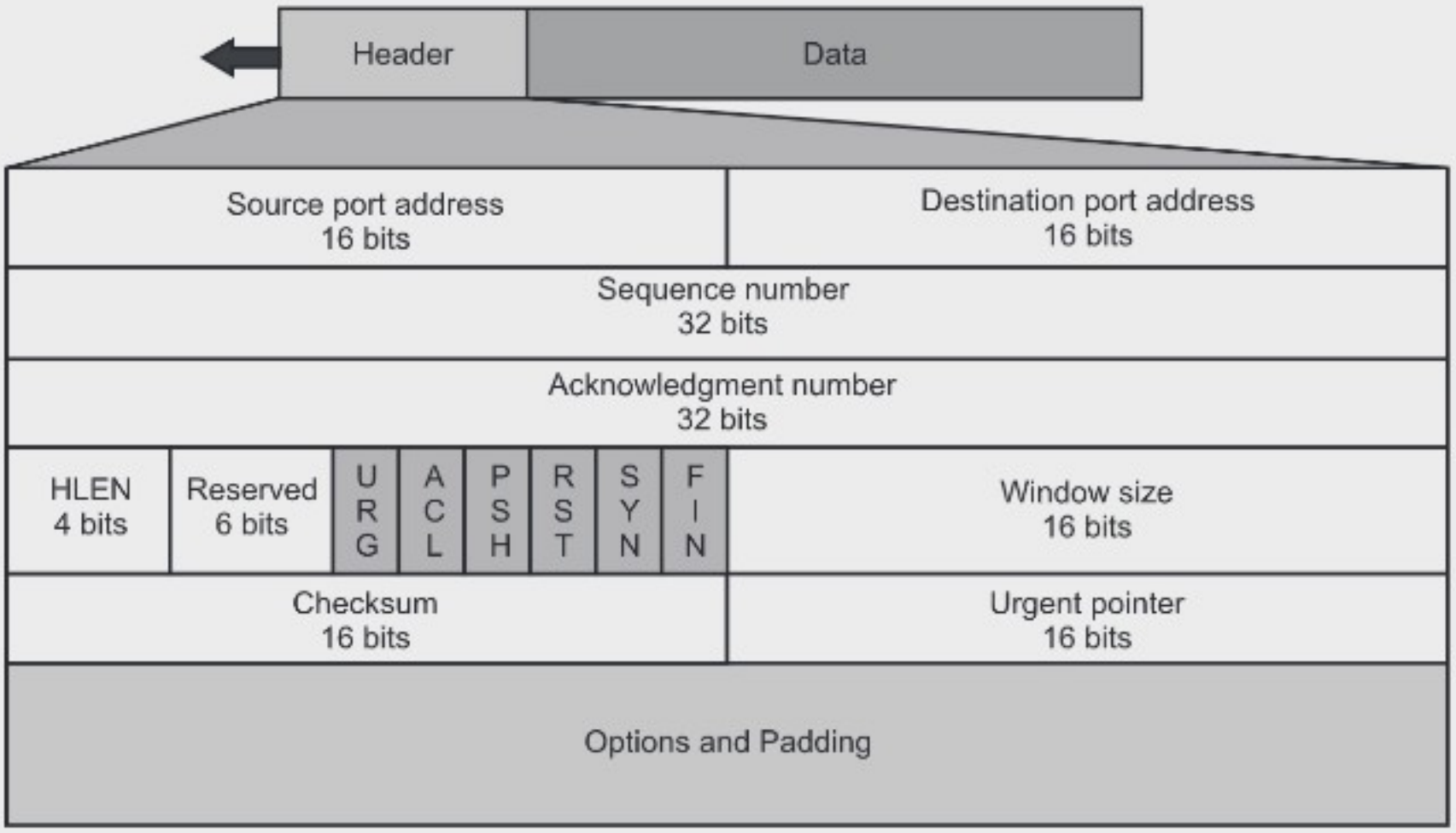


Fig. 6.10: TCP Segment Format

3. **Sequence number:** This 32 bit field defines the number assigned to the first byte of data contained in the segment.
4. **Acknowledgement number:** This 32 bit field defines the byte number that the receiver of the segment is expecting to receive from another party.
5. **Header length:** This 4 bit field defines the length of the header. The length of the header can range between 20 to 60 bytes.
6. **Reserved:** This 6 bit field is reserved for future use.
7. **Control:** This field defines 6 different control bits or flags as shown in Fig. 6.11. One or more flags can be set at a time.

Note: URG: Urgent pointer is valid
ACK: Acknowledgement is valid
PSH: Request for push
RST: Reset the connection
SYN: Synchronize sequence number
FIN: Terminate the connection

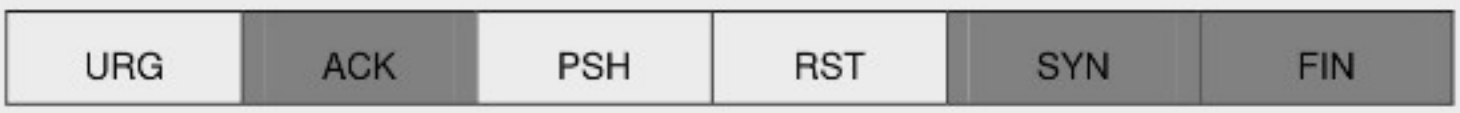


Fig. 6.11: Control Fields

- These bits enable flow control connection establishment and termination, connection abortion, and the mode of data transfer in TCP.
- The brief description of each bit is shown in Table 6.3.

Table 6.3: Description of flage in the control field

Flag	Description
URG	The value of the urgent pointer field is valid.
ACK	The value of the acknowledgment field is valid.
PSH	Push the data.
RST	Reset the connection.
SYN	Synchronize sequence number during connection.
FIN	Terminate the connection.

8. **Windows Size:** This 16 bit field defines the size of the window in bytes that other parties must maintain. It is used for flow control between two stations and indicates the amount of buffer (in bytes) the receiver has allocated for a segment, i.e. how much data is the receiver expecting.
9. **Checksum:** This 16 bit field contains the checksum used for error control.
10. **Urgent Pointer:** This 16 bit field is valid only if the urgent flag is set, it is used when the segment contains urgent data.
11. **Option:** There can be up to 40 bytes of optional information in the TCP header. It facilitates additional options which are not covered by the regular header. Option field is always described in 32-bit words. If this field contains data less than 32-bit, padding is used to cover the remaining bits to reach 32-bit boundary.

6.7 TCP VS UDP

- Following Table Shows the Difference between TCP and UDP:

Table 6.4: Difference between TCP and UDP

Sr. No.	Terms	TCP	UDP
1.	Acronym for	Transmission Control Protocol.	User Datagram Protocol.
2.	Connection	TCP is a connection-oriented protocol.	UDP is a connectionless protocol.
3.	Speed of transfer	The speed for TCP is slower than UDP.	UDP is faster because there is no error-checking for packets.
4.	Header Size	TCP header size is 20 bytes.	UDP Header size is 8 bytes.
5.	Weight	TCP is heavy-weight. TCP requires three packets to set up a socket connection, before	UDP is lightweight. There is no ordering of messages, no tracking connections,

		any user data can be sent. TCP handles reliability and congestion control.	etc. It is a small transport layer designed on top of IP.
6.	Data Flow Control	TCP does Flow Control. TCP requires three packets to set up a socket connection, before any user data can be sent. TCP handles reliability and congestion control.	UDP does not have an option for flow control.
7.	Error Checking	TCP does error checking	UDP does error checking, but no recovery options.
8.	Reliability and Acknowledgements	Unreliable best-effort delivery without acknowledgements.	Reliable delivery of messages all data is acknowledged.
9.	Retransmissions	Not performed. Application must detect lost data and retransmit if needed.	Delivery of all data is managed, and lost data is retransmitted automatically.
10.	Overhead	Very low	Low, but higher than UDP.
11.	Data Quantity Suitability	Small to moderate amounts of data.	Small to very large amounts of data.

6.8 DOMAIN NAME SYSTEM (DNS)

- The three top services provided by the application layer for smooth functioning of different applications are:
  - Network Security
  - Domain Name System (DNS)
  - Network Management
- Domain Name System (DNS) is one of the supporting program of the client server network that is used to handle the addressing and naming within the internet. DNS is a host name to IP address translation service. DNS is a distributed database implemented in a hierarchy of name servers.

Need of DNS:

- A user of an e-mail program may know the e-mail address of the recipient, however the IP protocol (of TCP/IP model) needs the IP address. The DNS client program sends a request to a domain name server to map the e-mail address to the corresponding IP address.

- It is also important to understand that every remote device (host in network) will have an alias name. To identify an entity, TCP/IP protocol will use the IP address, which uniquely identifies the connection of a host (any remote device) to the Internet.
- However, people prefer to use names instead of numeric addresses (for simplicity). Therefore, we need a system that can map a name to an address or an address to a name. So this entity is called DNS (Domain name system).
- This service will not be directly used by the end user, there is an application program for carrying out this mapping (of the alias and the IP address) work .

Working of DNS

- DNS is a client/server network communication protocol. DNS clients send requests to the server while DNS servers send responses to the client.
- Client requests contain a name which is converted into an IP address known as a forward DNS lookups while requests containing an IP address which is converted into a name known as reverse DNS lookups.
- DNS implements a distributed database to store the name of all the hosts available on the internet.
- If a client like a web browser sends a request containing a hostname, then a piece of software such as DNS resolver sends a request to the DNS server to obtain the IP address of a hostname.
- If a DNS server does not contain the IP address associated with a hostname, then it forwards the request to another DNS server. If the IP address has arrived at the resolver, which in turn completes the request over the internet protocol.

6.8.1 Namespace in DNS

- The alias names that are assigned to each remote host in the network should be unique, so it should be selected carefully from the namespace. A namespace that maps each address to a unique name can be organized in two ways:
  1. Flat Namespace
  2. Hierarchical Namespace

1. Flat Namespace

- In a flat namespace , a name is a sequence of characters without structure.
- A name in this space is assigned to an address.
- The names were convenient and short.
- The main disadvantage of a flat Namespace is that it can't be used in a large system like in the Internet because it must be centrally controlled in order to avoid any ambiguity and duplication.

2. Hierarchical Namespace

- In hierarchical namespace , each name consists of several parts.
- First part defines the nature of the organization, the second part defines the name of an organization, third part defines the department of the organization, and so on.

- In hierarchical namespace , the authority to assign and control the namespace s can be decentralized.
- Authority for names in each partition is passed to each designated agent.

Domain Namespace

- In order to have a hierarchical namespace , a domain Namespace was designed.
- DNS is a protocol that can be used on different platforms.
- In this design the names are basically defined in an inverted-tree structure with the root at the top.
- The tree can have only 128 levels i.e. level 0 (root) to level 127.
- Domain Namespace is divided into different sections in the Internet: Generic domain, country domain.
- The generic domain can be of different types i.e. com (commercial), edu (educational institutions), gov (government), int (international organization), mil (military), net (network providers), and org (non-profit organizations).
- The country domains generally include one entry for every country. Also each domain is named by following an upward path.
- Each node in the tree has a label and it can be specified using 63 characters. It is very difficult for us to remember the string of numbers (ip addresses) and that is where domain names comes into picture.
- A domain is typically a subtree of the domain namespace . The name of any domain is the domain name of the node at the top of the subtree. A domain can be further divided into subdomains.
- The following Figure. 6.12 shows domain names and labels.

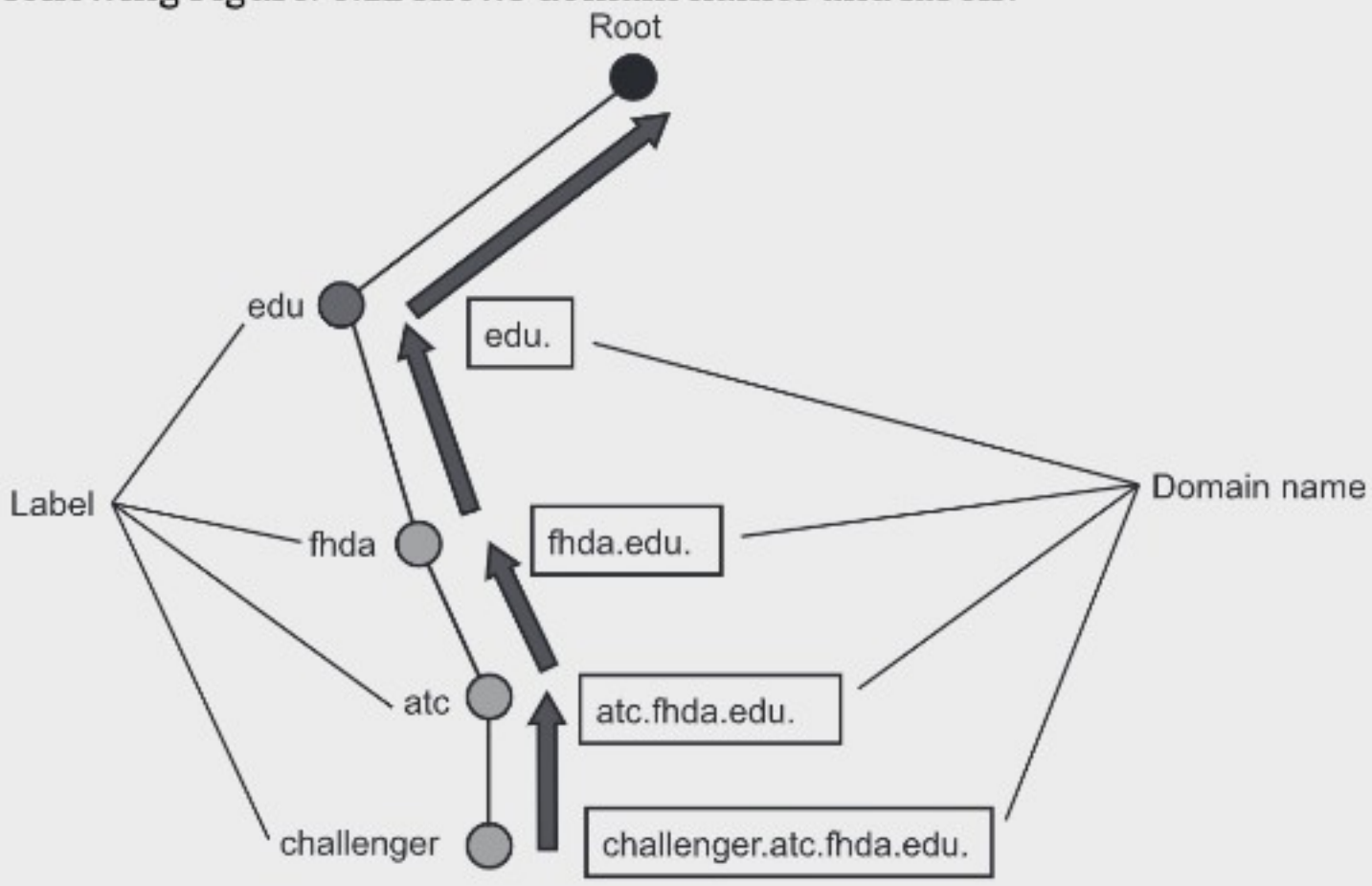


Fig. 6.12: Domain names and labels

6.8.2 Distribution of Namespace

- The information contained in any domain Namespace must be stored.
- However, it is very inefficient and also unreliable to have only one computer store such a huge amount of information. Failure of any one computer can make the data accessible.
- The simple solution to these problems is to distribute the information among many computers called DNS servers.

Hierarchy of Name Servers

- One way to implement this is to divide the whole space into many domains based on the first level.
- Name server contains the DNS database i.e. various names and their corresponding IP addresses.
- DNS allows domains to be divided further into smaller domains (subdomains).
- The first level domains are further divided into smaller subdomains called the second level domains.
- The hierarchy of the servers will be the same as that of the names.

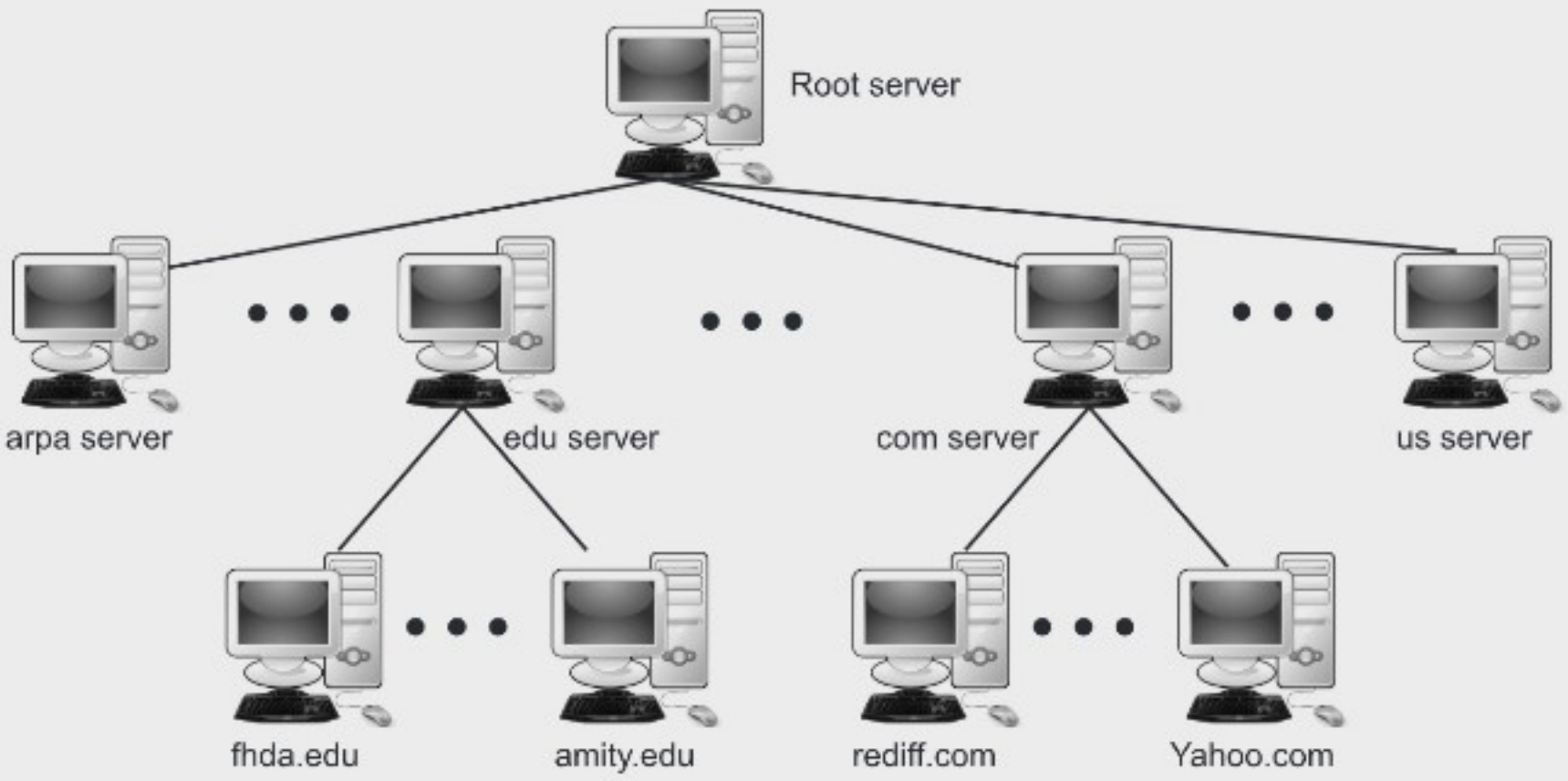


Fig. 6.13 : Hierarchy of name servers

Zones:

- We need to define the area over which each server has an authority. This restricted region over which a particular server has authority is called a zone.
- The server makes a database called as zone file and it keeps all the information for every node under that domain.
- However, if any server divides its domain into sub domains and delegates part of its authority to other servers, domain and zone refers to different things.

- The information about the nodes in the sub domains is further stored in the servers at the lower levels, with the original server keeping some sort of reference to these lower-level servers.

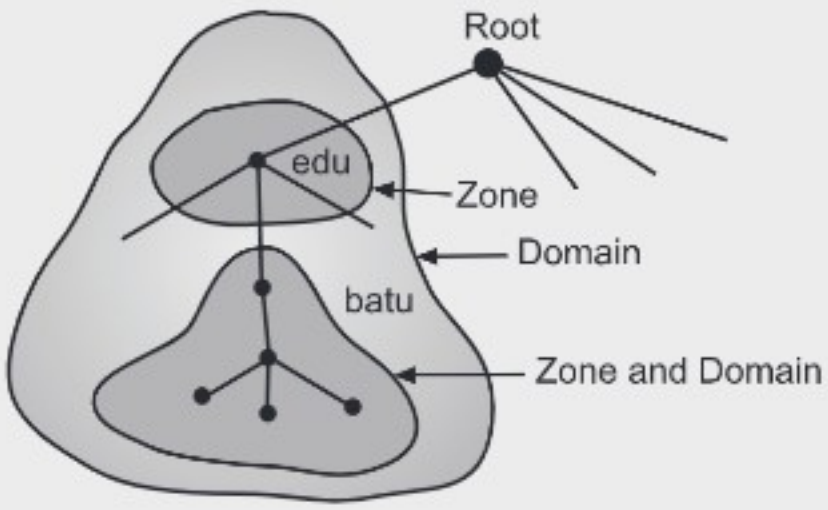


Fig. 6.14: Zones and domains

Root Server:

- This refers to the zone consisting of the whole DNS tree.
- It only keeps the reference of these servers.
- There are several root servers, each covering the whole domain namespace .
- The servers are distributed all around the world.
- DNS defines two types of servers namely primary and secondary servers.

1. **Primary servers:**

- This type of server stores files about its zone. It has the authority to create , update and delete any zone file and store it in a local disc.

2. **Secondary Servers:**

- This server transfers complete information about a zone from another server which may be primary or secondary server . The transferred information will be then stored in disc storage. It is not authorized to create and update a zone file.

Zone Transfer:

- A primary server loads all information from the disk file; the secondary DNS Server loads all information from the primary server.
- When the secondary downloads information from the primary, it is called zone transfer.

6.8.3 DNS in the Internet

- We will now understand how the DNS is implemented on the internet. In the Internet, the domain Namespace (tree) is divided into three different sections: generic domains, country domains, and the inverse domain.

1. **Generic Domain**

- The first level the of generic domain section allows 14 possible values. The generic domains define registered hosts according to their generic behavior. for example, we have edu for education etc.

Table 6.5: Domain Name with discription

Label	Description
aero	Airlines and aerospace companies
biz	Businesses or firms (similar to "com")
com	Commercial organizations
coop	Cooperative business organizations
edu	Educational institutions
gov	Government institutions
info	Information service providers
int	Information service providers
mil	Military groups
museum	Museums and other nonprofit organizations
name	Personal names (individuals)
net	Network support centers
org	Nonprofit organizations
pro	Professional individual organizations

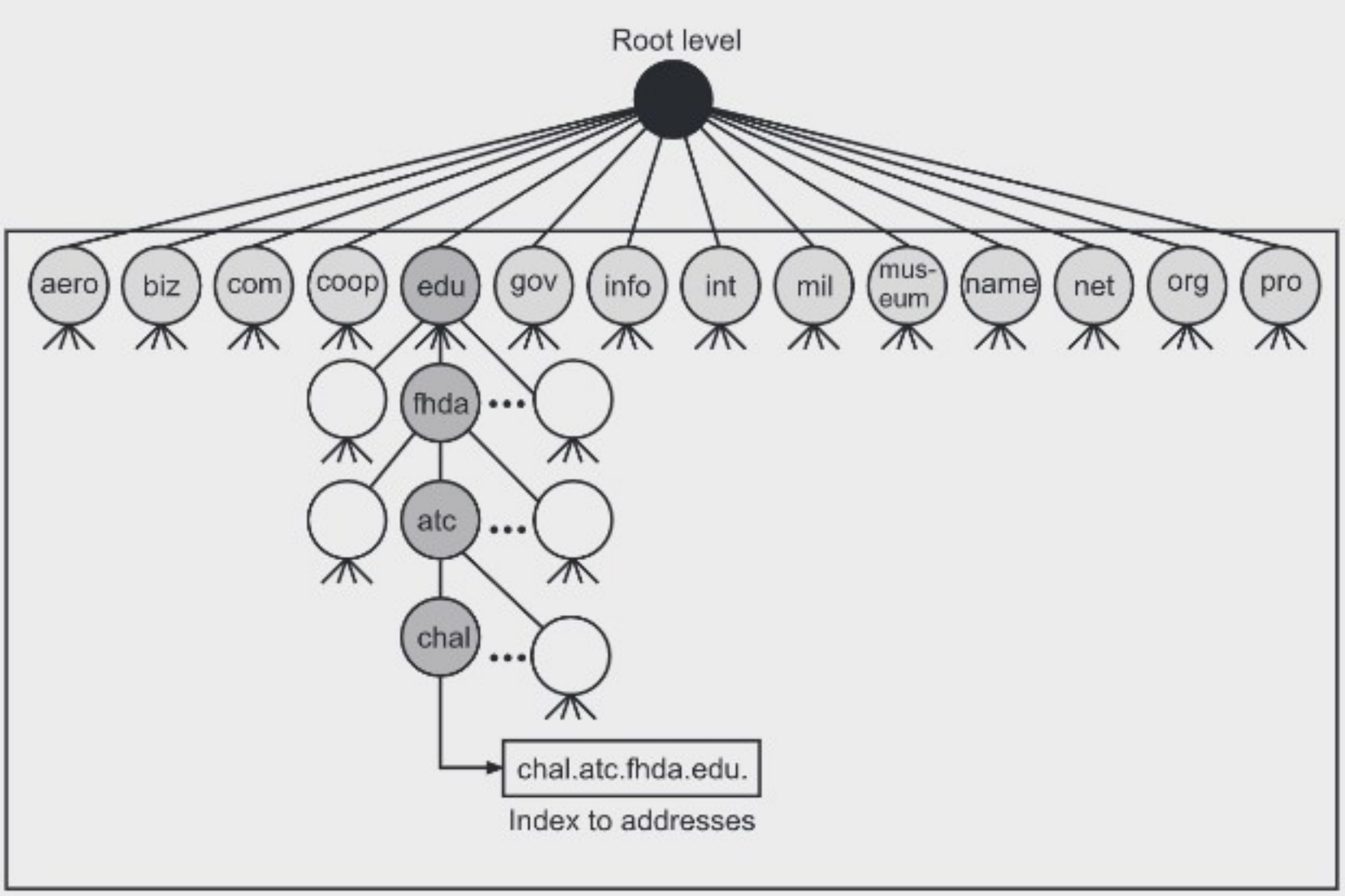


Fig. 6.15: Generic domains

2. Country Domain

- This domain uses two characters country abbreviations e.g. US for united states. Second label in this domain specifes organization or national designations.
- **For example,** for Australia the country domain is “au”, India is ".in", UK is ".uk" etc.

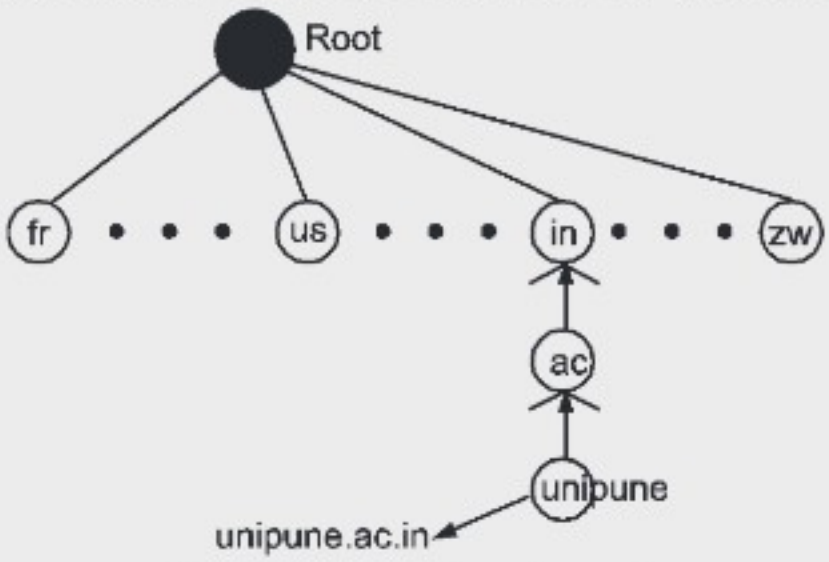


Fig. 6.16: country domain

3. Inverse Domain

- This is used for mapping an address to a name.

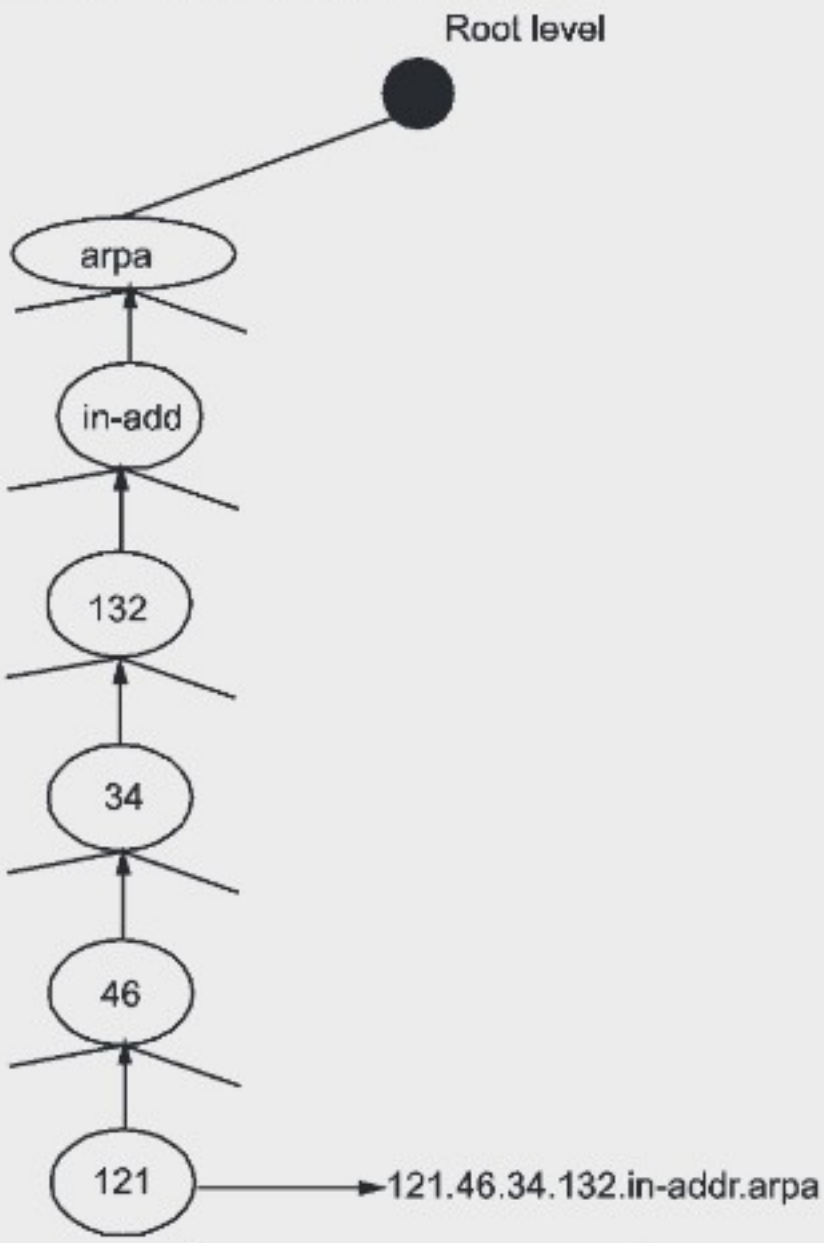


Fig. 6.17: Inverse Domain

- This may happen, for example, when a server has received a request from a client to do a task. Although the server has a file that contains a list of authorized clients, only the IP address of the client (extracted from the received IP packet) is listed.
- The server then asks its resolver to send a query to the DNS server to map an address to a name in order to determine if the client is on the authorized list.
- This is exactly opposite to the process of mapping a name to an address.

Name Address Resolution:

- The process of mapping a name to address and vice versa is called as name address resolution

6.9 E-MAIL – ARCHITECTURE

Architecture

- One of the most popular Internet services is electronic mail (e-mail). This application program will become popular that the designers of the Internet probably never imagined. Its architecture consists of several components. At the beginning of the Internet era, the messages sent by electronic mail were short and consisted of text only; they allowed people to exchange quick memos.

E-mail architecture consists of three components:

- User Agent (UA)
- Message Transfer Agent (MTA)
- Message Access Agent (MAA)

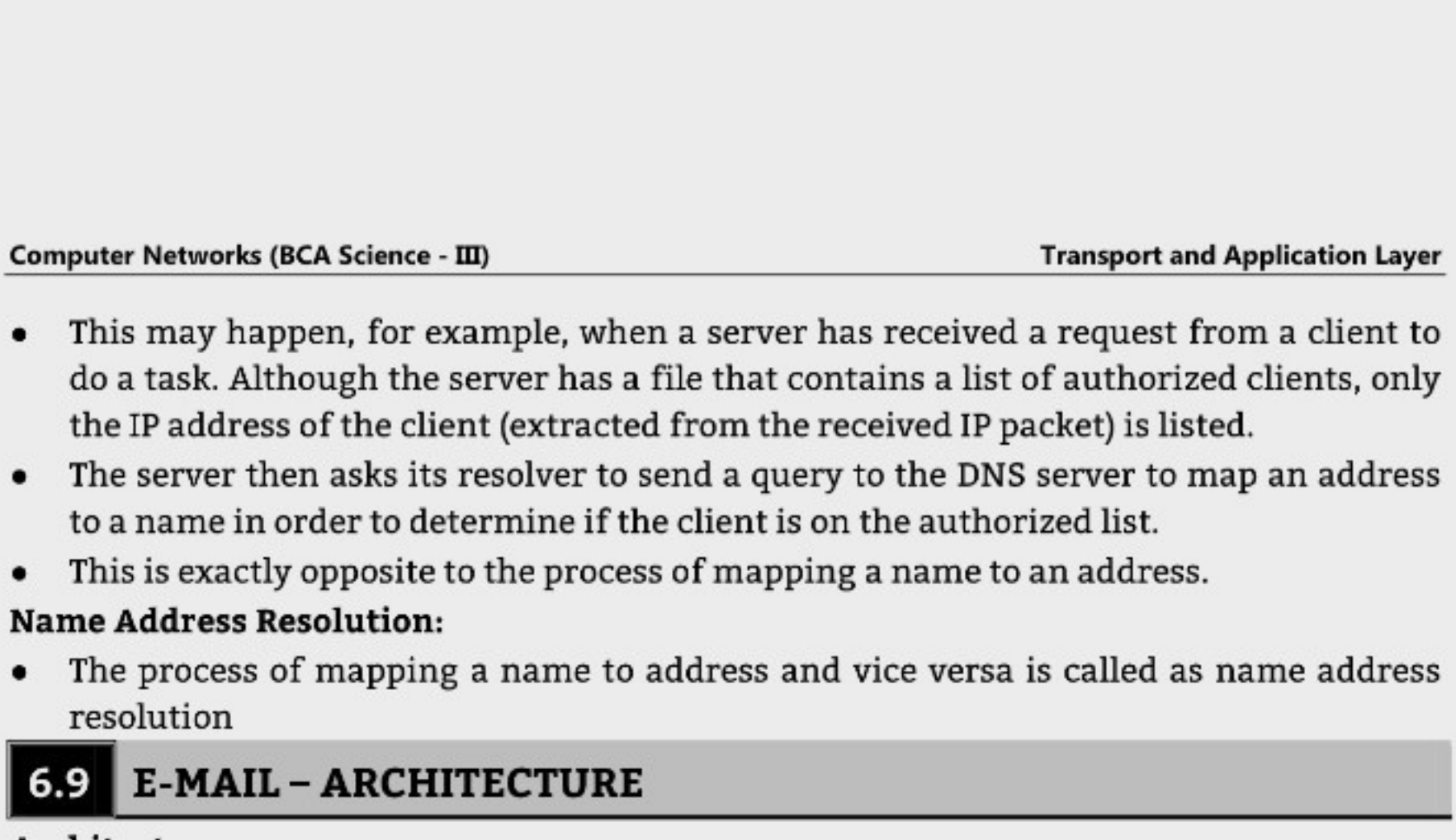


Fig. 6.18: E-mail Architecture

6.9.1 User Agent

- A user agent is a Package or program of a software that composes, reads, responds to and forward messages. It also handles user computers with local mailboxes.
- Services Provided by User Agent are shown in the following Fig. 6.19 .

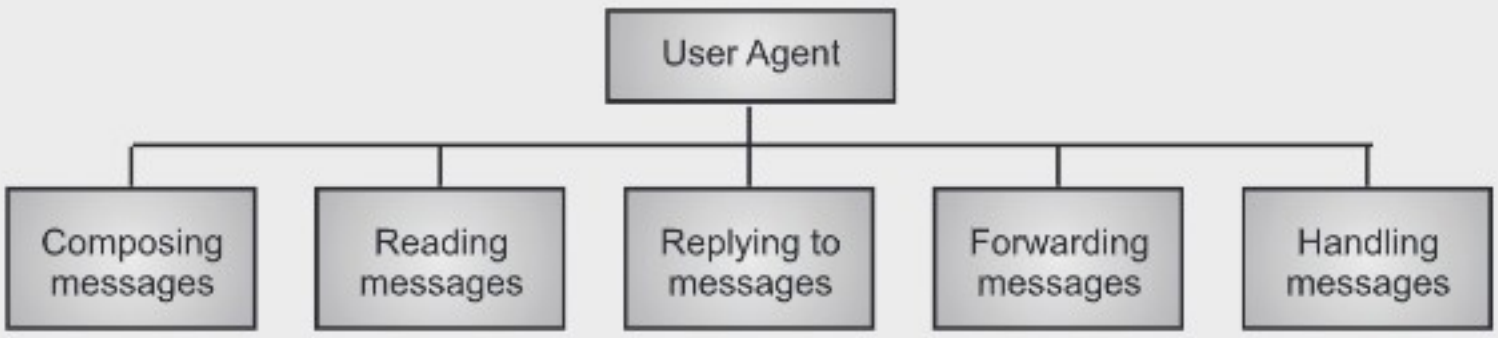


Fig. 6.19: Services of user agent

- **Composing Messages:** A user agent helps the user to compose the e-mail message by providing a template on the screen to be filled in by the user. Some have a built-in editor facility that can do spell checking, grammar checking, and other tasks etc .
- **Reading Messages:** The another task of the user agent is to read the incoming messages. When a user invokes a user agent, it first checks the mail in the incoming mailbox. Most user agents show a one-line summary of each received mail. Each e-mail contains the following fields.
  1. A number field.
  2. A flag field that shows the status of the mail such as new, already read but not replied to, or read and replied to.
  3. The size of the message.
  4. The sender.
  5. The optional subject field.
- **Replying to Messages:** A user agent usually allows the user to reply to the original sender or to reply to all recipients of the message. The reply message may contain the original message (for quick reference) and the new message. Replying is defined as sending a message to the sender or recipient of the copy.
- **Forwarding Messages:** Forwarding is defined as sending the message to a third party. A user agent allows the receiver to forward the message, with or without extra comments, to a third party.

Handling Mail Boxes:

- A user agent creates two mail boxes i.e., inbox and outbox.
- Inbox keeps all the received e-mails until they are deleted by the user. The outbox keeps all the sent e-mails until the user deletes them.
- There are two types of user agents: command-driven and GUI-based.

- **Command-Driven**: A command-driven user agent normally accepts a one-character command from the keyboard to perform its task. For example, a user can type the character r, at the command prompt, to reply to the sender of the message, or type the character R to reply to the sender and all recipients. Some examples of command-driven user agents are mail, pine, and elm.
- **GUI-Based Modem user agents:** They contain graphical-user interface (GUI) components that allow the user to interact with the software by using both the keyboard and the mouse. Some examples of GUI-based user agents are Eudora, Microsoft's Outlook, and Netscape

Sending Mail:

- In order to send mail, the user creates mail through the user agent which looks very similar to Postal Mail. E-mail has an envelope and a message as shown in Fig. 6.20.
- The envelope contains sender and receiver addresses. Message contains header and body. In header sender, receiver, date, subject of e-mail are defined. Body part contains actual information to be read by the recipient.

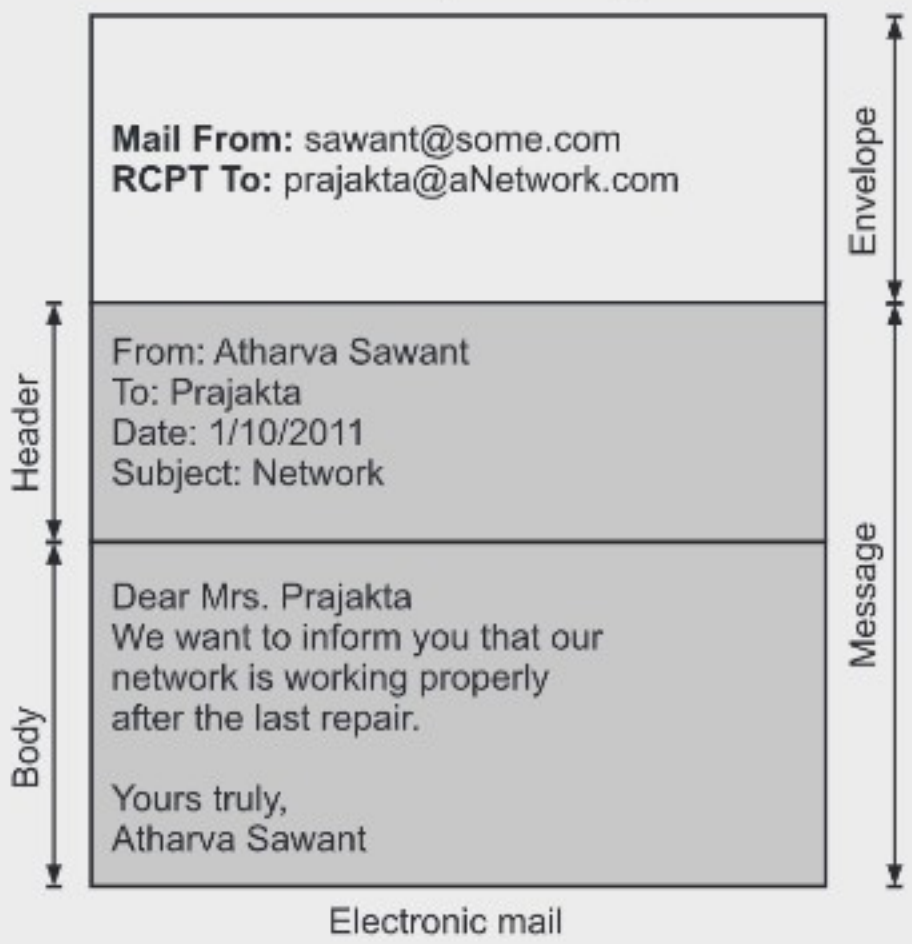


Fig. 6.20: Format of e-mail

Receiving Mail:

- The User agent, or a timer, is triggered by the User. Where a user has mail, the user agent will notify the user with a notice if the user is ready to read the mail, a list will be shown in which each line includes a description of a particular message's mailbox information.

Addresses:

- A mail handling system must use a system address with unique addresses to deliver mails. Each user has a unique e-mail address which is selected the time a person signs up for an e-mail ID.
- E-mail address contains two parts, local port and a domain name, separated by @ sign.

Fig. 6.21: E-mail address

- Local port defines the name of the user mailbox. And the domain name defines the name of the mail server.

Mailing List or Group List:

- Electronic mail allows for the one name, an alias, to represent several different e-mail addresses; this is called a mailing list. The system checks the name of the recipient against the alias database whenever a message is to be sent; if there is a mailing list for the defined alias, separate messages, one for each entry in the list, must be prepared and given to the MTA.

MIME:

- Multipurpose Internet Mail Extensions (MIME) is a protocol that allows non-ASCII data to be sent through e-mail.
- E-mail system has one limitation, it can send messages only in NVT 7-bit ASCII. It cannot be used for languages like German, Russian, Chinese, Japanese and Hebrew. Also it cannot be used to send binary files or video or audio data.
- MIME transforms non-ASCII data at the sender site to NVT ASCII and delivers them to the client MTA to be sent through the Internet. The message at the receiving site is transformed back to the original data.

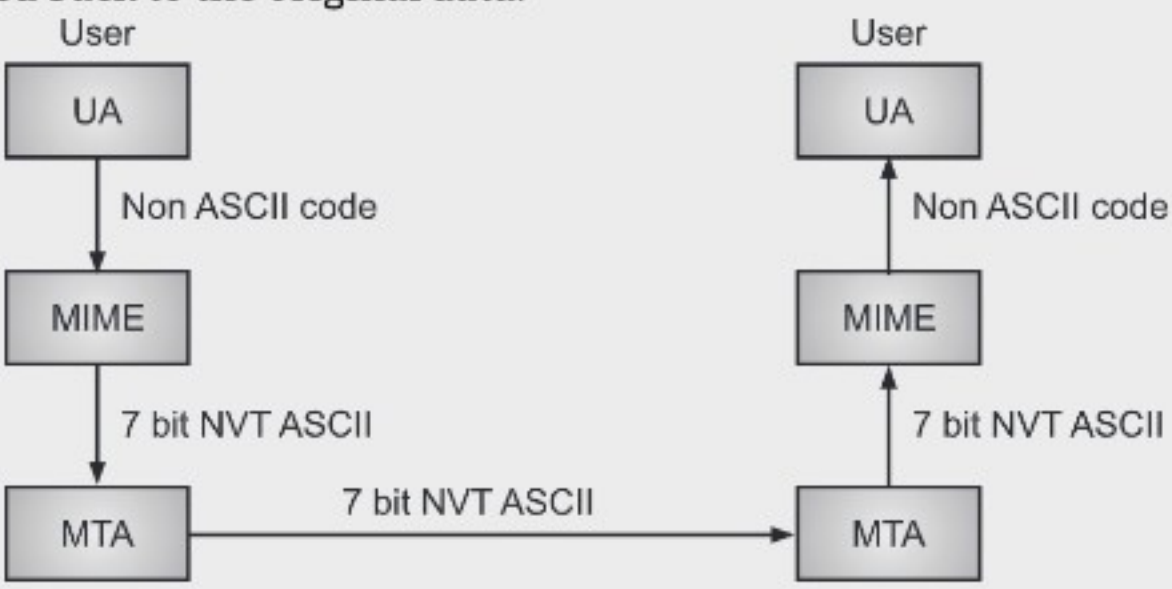


Fig. 6.22: MIME

6.9.2 Message Transfer Agent "MTA"

- The actual mail transmission is done through MTAs. A system must have the client MTA for sending mail, and a system must have a server MTA for receiving mail.
- Simple Mail Transfer Protocol "SMTP" is the formal protocol that defines the MTA client and server within the internet.
- SMTP is used in the first and second phases of mail delivery.
- SMTP is not involved in the third stage, however, as SMTP is a push protocol; it transmits the client's message to the server. The path of the bulk data "messages" is from client to server, in other words.
- On the other hand, a pull protocol is required for the third stage. The client must use the server to pull messages. The direction from the server to the client for the bulk data is the third stage that uses an agent for accessing messages.
- There are currently two protocols for accessing messages: Post Office Protocol version 3 "POP3" and Internet Mail Access Protocol "IMAP".

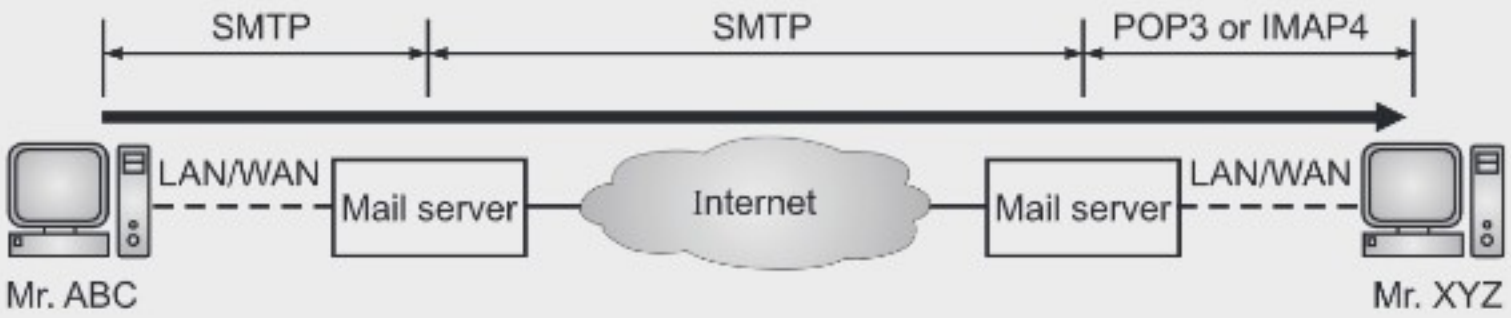


Fig. 6.23: Protocols of MTA

6.9.2.1 Simple Mail Transfer Protocol (SMTP)

- SMTP is used two times, between the sender and the sender's mail server and between the two mail servers. SMTP simply defines how commands and responses must be sent back and forth between an MTA client and an MTA server.

Commands and Responses:

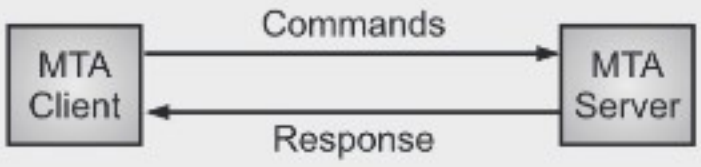


Fig. 6.24: SMTP

- Commands are sent by client to server. Command consists of a keyword followed by zero or more arguments. SMTP uses 14 commands. The first five are mandatory; every implementation must support these five commands. The next three are often used and highly recommended. The Last six are seldom used.
- Responses are sent from server to client. A response is a three digit code.
- Table 6.6 shows SMTP commands.

Table 6.6: SMTP Commands

Keyword	Argument (s)
HELO	Sender's host name
MAIL FROM	Sender of the message
RCPT TO	Intended recipient of message
DATA	Body of the mail
QUIT	-
RSET	-
VRFY	Name of recipient to be verified
NOOP	-
TURN	-
EXPN	Mailing list to be expanded
HELP	Command name
SEND FROM	Intended recipient of the message
SMOL FROM	Intended recipient of the message
SMAL FROM	Intended recipient of the message

Table 6.7: SMTP Responses

Code	Description
Positive Completion Reply	
211	System status or help reply
214	Help message
220	Service ready
221	Service closing transmission channel
250	Request command completed
251	User not local, the message will be forwarded
Positive Intermediate Reply	
354	Start mail input
Transient Negative Completion Reply	
421	Service is not available
450	Mailbox not available
451	Command aborted: local error
452	Command aborted: insufficient storage

Permanent Negative Completion Reply	
500	Syntax error, unrecognized command
501	Syntax error in parameters or arguments
502	Command not implemented
503	Bad sequence of commands
504	Command temporarily not implemented
550	Command is not executed, mailbox unavailable
551	User not local
552	Requested action aborted, exceeded storage location
553	Requested action not taken, mailbox name not allowed
554	Transaction failed.

Mail Transfer Phases:

- Mail transfer occurs in three phases: connection establishment, mail transfer and connection termination.
- Now, let us see the typical SMTP procedure with an example:

```
$ telnet mail.gmail.com 25
Trying 70.168.78.100….
connected to mail.gmail.com (70.168.78.100).
…….Connection Establishment……
220 mta 13.gmail.com SMTP server ready Monday,15 Apr. 2020…
HELO mail· gmail.com
250 mta 13.rediffmail.com
…….Mail Transfer……
MAIL FROM: 250 sender <abc@gmail.com> OK
RCPT TO: xyz@gmail.com
 250 Recipient <xyz@gmail.com> OK
                                DATA
354 OK send data ending with <CRLF>.<CRLF>
FROM: ABC
TO: XYZ
Hi, How are you ?
…….Connection Termination……
250 message received: mail@gmail.com
QUIT
221 mta 13.gmail.com SMTP server closing connection
Connection closed by foreign host.
```

6.9.2.2 Web Mail, Web based E-mail

- E-mail is such a common application that some websites today provide this service to anyone who access the site. Three common sites are rediff, Yahoo, and Google.
- In web-based mail transfer from sender's browser to mail server through HTTP.
- Transfer of message from sending mail server to receiving server still through SMTP.
- Message from receiving server (web server) to receiver browser is done through HTTP.
- Instead of POP3 and IMAP4, HTTP is used as MAA.
- The idea is very simple. Let us go through two cases:

Case I:

- Mr.ABC, the sender, uses a conventional mail server in the first case; Mr. XYZ, the recipient, has a Web based server account in it. Mail transfer is done via SMTP from Mr.ABC's browser to their mail server. The message being transmitted from the sending mail server to the receiving mail server is still via SMTP. However, the message to Mr. XYZ's browser from the receiving server (the web server) is done via HTTP. In other words, the HTTP is typically used instead of using POP3 or IMAP4. If Mr. XYZ wants to get his e-mails recovered, he sends an HTTP request message to the website (for example, gmail). The website sends a form for Mr. XYZ to fill in, which contains the user name and password. If the log-in name and password match, the e-mail list is transferred in HTML format from the Web server to Mr. XYZ's browser. Now Mr. XYZ can browse through his received e-mails and then can get his e-mails one by one using more HTTP transactions.

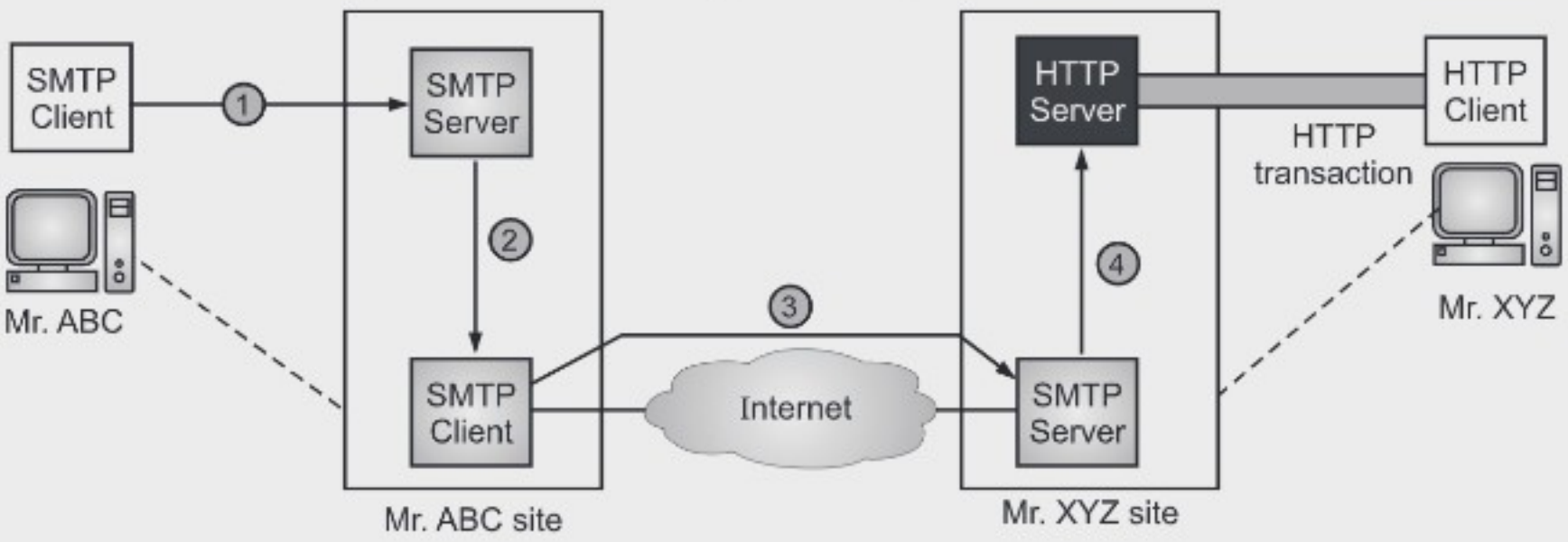


Fig. 6.25: Web based e-mail, Case I

Case II:

- Both Mr. ABC and Mr. XYZ use Web servers in the second case but not exactly the same server. Using HTTP transfers Mr. ABC sends the message to the Web server. Mr. ABC sends an HTTP request message to its Web server using Mr. XYZ's mailbox

name and address as the URL. The Mr. ABC server passes the message to the SMTP client and sends it via SMTP protocol to the server at the Mr. XYZ site. Mr. XYZ receives the message using transactions running HTTP. The communication from the server at the Mr. ABC site to the server at the Mr. XYZ site, however, also happens using SMTP protocol.

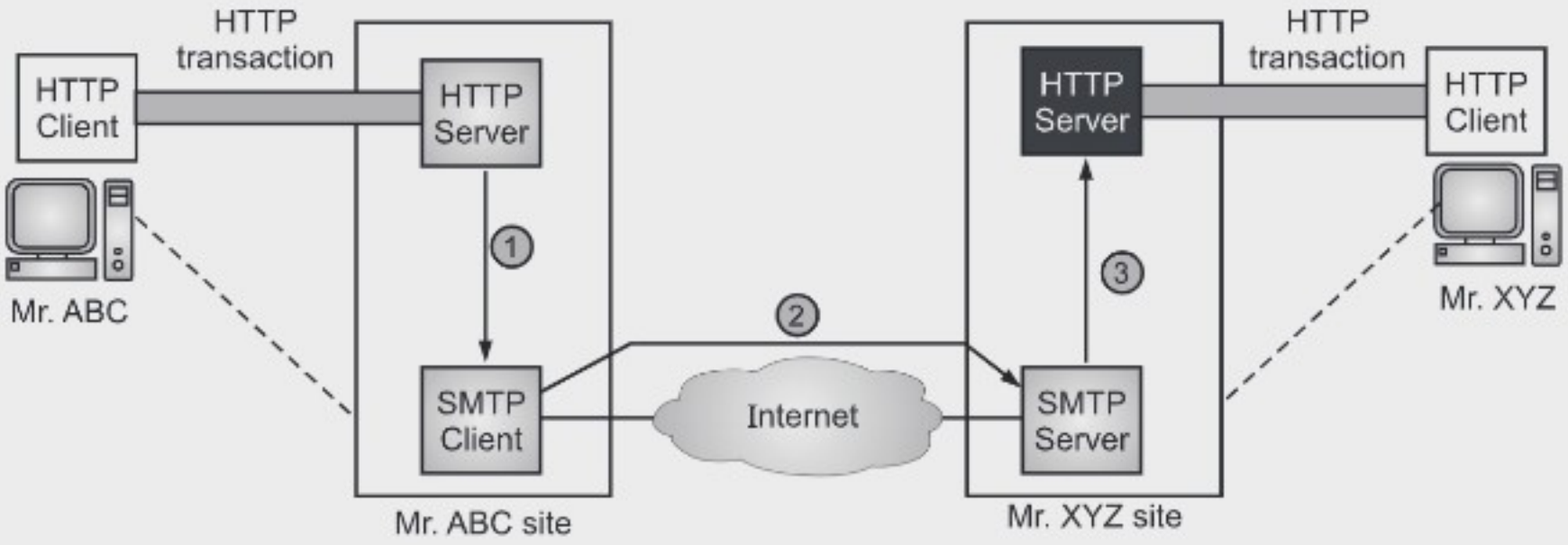


Fig. 6.26: Web based e-mail, Case II

6.10 WWW ARCHITECTURE

- World Wide Web was created by Timothy Berners Lee in 1989 at CERN in Geneva.
- It is a way of exchanging information between computers on the Internet, tying them together into a vast collection of interactive multimedia resources.
- It is a repository of information linked together from points all over the world. This information consists of text, graphics, audio and video etc. are connected by hyperlinks.
- WWW provides flexibility, portability and user friendly features.
- HTTP is a protocol, which is used to retrieve information from the web.

Architecture of WWW

- Initially, the WWW consisted of a two-tiered architecture: clients and servers.
- Client uses a browser software to access information stored on web server.
- Every web server contains one or more documents known as web pages.
- Each web page can contain a link to other page of the same site or other site (server). When a client needs some information from a particular server, it sends a request to that server.
- Server finds that information and send it to the client in the form of a web document.

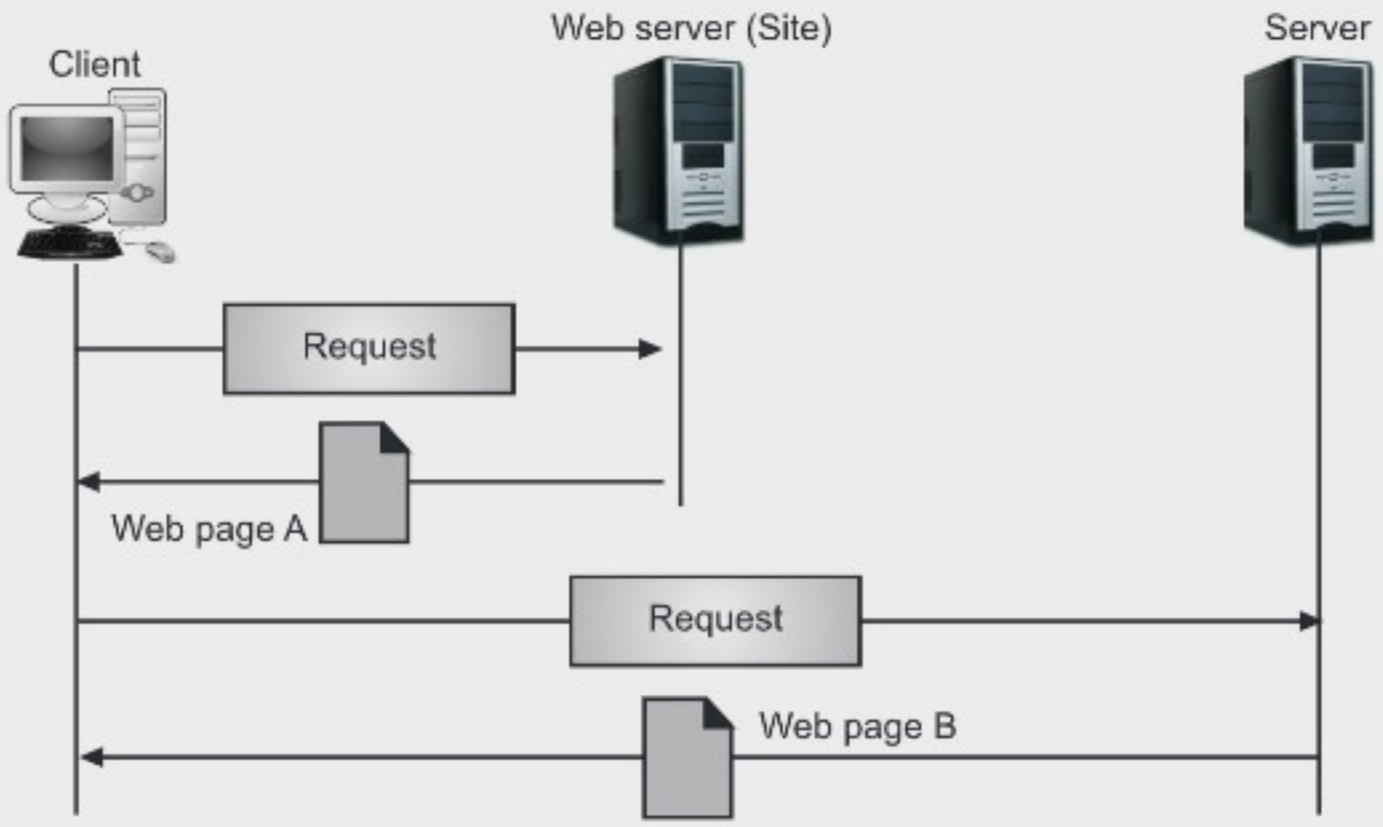


Fig. 6.27: Architecture of www

1. **Client (Browser):**

- Many vendors offer variety of browsers that interpret, almost all having the same architecture and display a web document.
- Every browser consists of three parts i.e., a controller, client protocol and interpreters.
- The controller receives input from keyboard or mouse and uses the client program to access the document. After that controller uses one of the interpreters which can be HTML,Java or Javascript, to display the document.

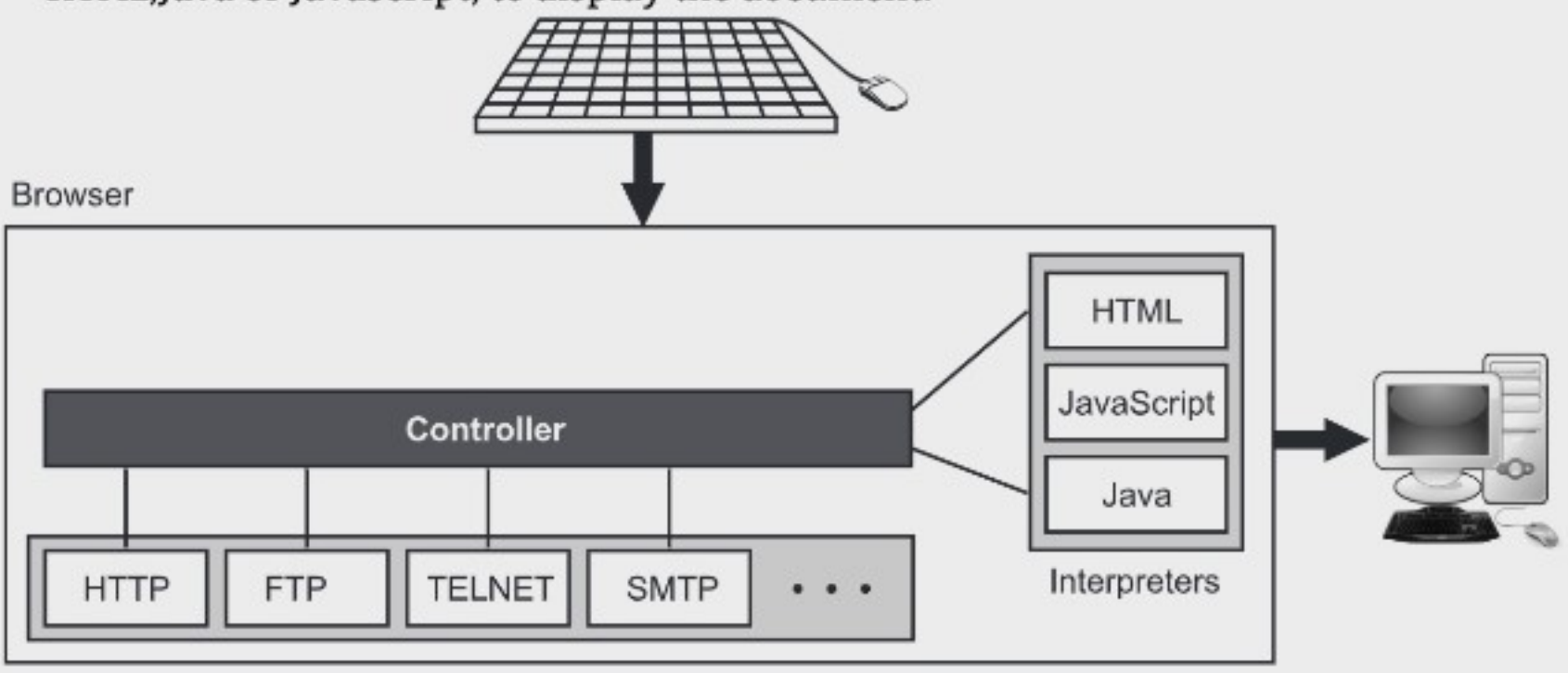


Fig. 6.28: Browser

2. **Server:**

- The web pages are stored on the server. When client request comes, the corresponding document is sent to the client.

- To improve efficiency, it uses cache or multi-threading or multiprocessing concepts.
- **Uniform Resource Locator (URL):** A client who wants to access web pages need an address known as a uniform resource locator (URL).
- The URL contains four things: Protocol, Host Computer, Port and Path as shown in following fig.

Fig. 6.29: URL (Uniform Resource Locator)

- The protocol is the client/server program used to retrieve the document. Many different protocols can retrieve a document; among them are FTP or HTTP.
- The host is the server on which information is stored.
- Port number gives port number of the server, it is optional. If the port is included, it is inserted between the host and the path, and it is separated from the host by a colon.
- Path is the path name of the file where the information is stored.
- For example: rediff.com/news, google.com etc.

3. Cookies:

- The www uses HTTP protocol, which is a client/server protocol. The World Wide Web was originally designed as a stateless entity. A client sends a request; a server responds. Their relationship is over.
- But today, the www has the functions like:
  - (a) Some websites need to allow access to registered clients only.
  - (b) Websites are used for e-commerce purposes.
  - (c) Some websites are used as portals.
  - (d) Some are just advertising.
- For these purpose, the cookie mechanism is used:
  - (i) A cookie is a small program which the server stores in the client machine to identify the client.
  - (ii) A cookie can be used for authenticating, session tracking, and remembering specific information about users.
  - (iii) An e-commerce website uses a cookie for its client shoppers. When a client selects an item and inserts it into cart, the cookie contains information about that item.
  - (iv) Cookie is also used by advertising agencies.

6.11 HTTP – HTTP TRANSACTION

HTTP Transaction:

- The HyperText Transfer Protocol (HTTP) is a main protocol used to access data on WWW.
- It defines a mechanism for communication between browser and the web server.

- It is also called request and response protocol because the communication between browser and server takes place in request and response pairs.
- Every HTTP message sent from a Web browser to a Web server is classified as an HTTP request, whereas every message sent from a Web server to a Web browser is classified as an HTTP response.
- A transaction refers to a single HTTP request and the corresponding HTTP response.
- HTTP is often referred as a stateless protocol.
- The following figure shows HTTP transaction between the client and server.

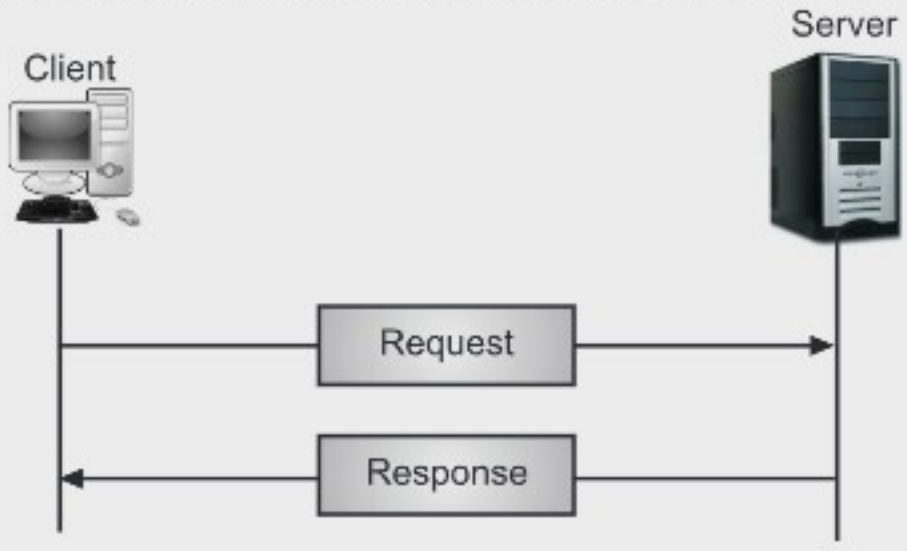
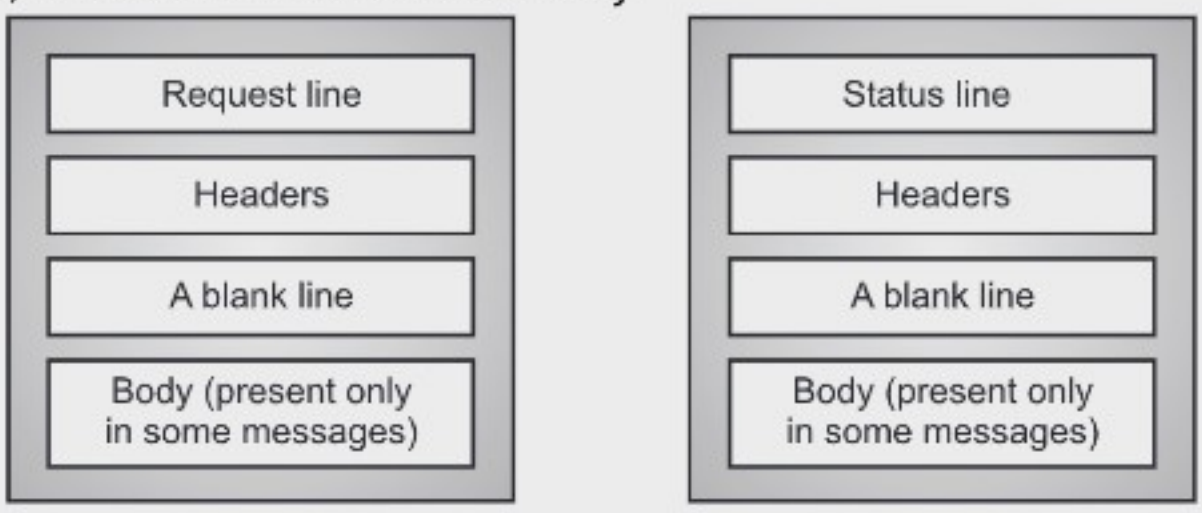


Fig. 6.30: HTTP transaction

- The format of request and response messages are similar. Request messages consist of request line, a header and sometimes a body. A response message consists of a status line, a header and sometimes a body.

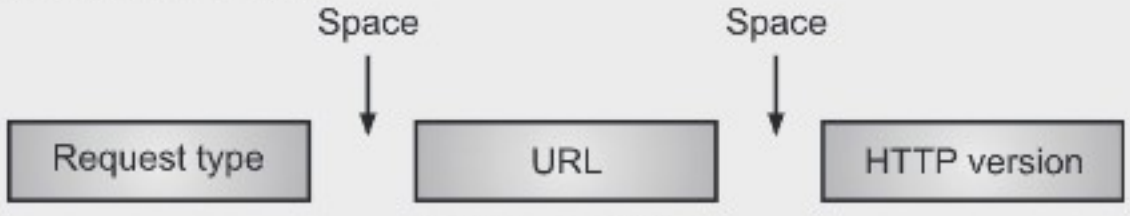


(a) Request message **(b) Response message**

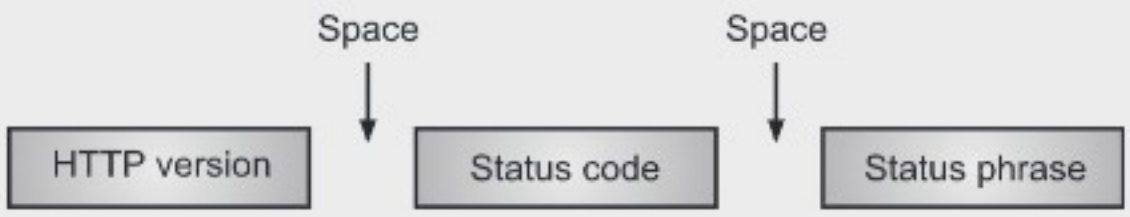
Fig. 6.31 : Request and response messages

Request and Status Lines:

- The first line in the request message is called a request line, the first line in response message is called status line.



(a) Request line



(b) Status line

Fig. 6.32: Request and status line

Request Type:

- The request type is categorized into methods. Some methods are:
  1. **GET:** To retrieve a document from the server.
  2. **HEAD:** Request information about a document but not the document itself.
  3. **POST:** Sends some information from the client to the server.
  4. **PUT:** Sends a document from the server to the client.
  5. **TRACE:** Echoes the incoming request.
  6. **CONNECT:** Reserved.
  7. **PATCH:** It contains a list of differences which should be implemented in the existing file.
  8. **MOVE:** Moves a file to another location.
  9. **OPTION:** Inquires about available options.
  10. **URL:** URL of web documents.
  11. **Version:** The current version of HTTP is 1.1.
  12. **Status code:** This field is used in the response message.
- It is similar to FTP and SMTP. It consists of three digits. The codes starting from 1 is informational, 2 are success, 3 are redirection, 4 are client error and starting from 5 are server error.

Header:

- The header exchanges information between client and server. Each header line has a header name, a colon, a space and header value.

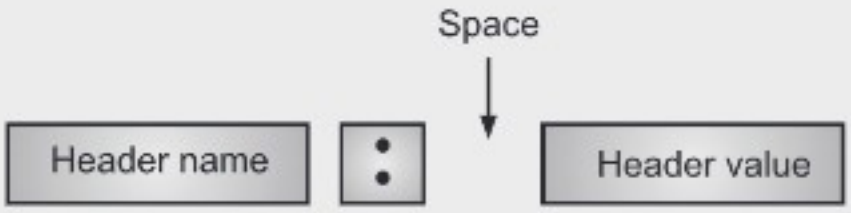


Fig. 6.33: Header format

- Header is divided into four categories:
  1. **General Header:** General header gives general information about the message and present in request and response message.
  2. **Request Header:** It can present only in a request message. It specifies the client configuration and client's preferred document format.
  3. **Response Header:** It is present only in response messages. It specifies the server's configuration and special information about the request.
  4. **Entity Header:** Entity header gives information about the body of the document.

Body:

- The body can be present in a request or response message. It contains the document to be sent or received.
- For example:

(1) Client sends a GET request for an image file with the path/user /bin/image1. Request does not have a body. The response message contains the status line and four lines of header.

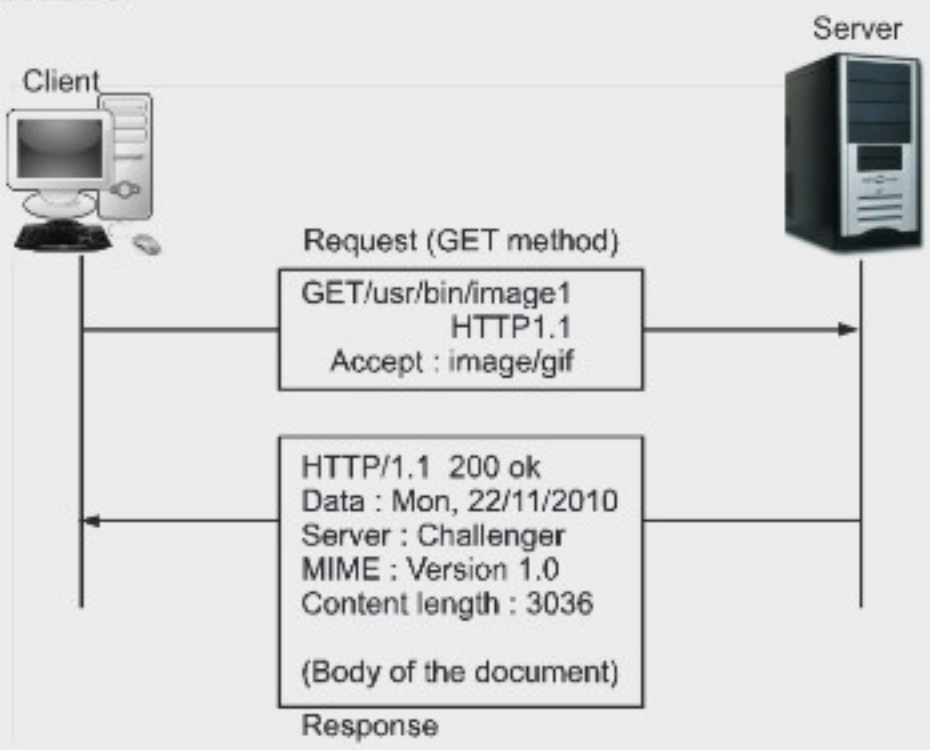


Fig. 6.34: HTTP transaction using GET method

(2) The client wants to send data to the server by using POST method. The request line shows the method (POST), URL and HTTP version(1.1). There are four lines of headers. The request body contains the input information. The response message contains the status line and four lines of headers.

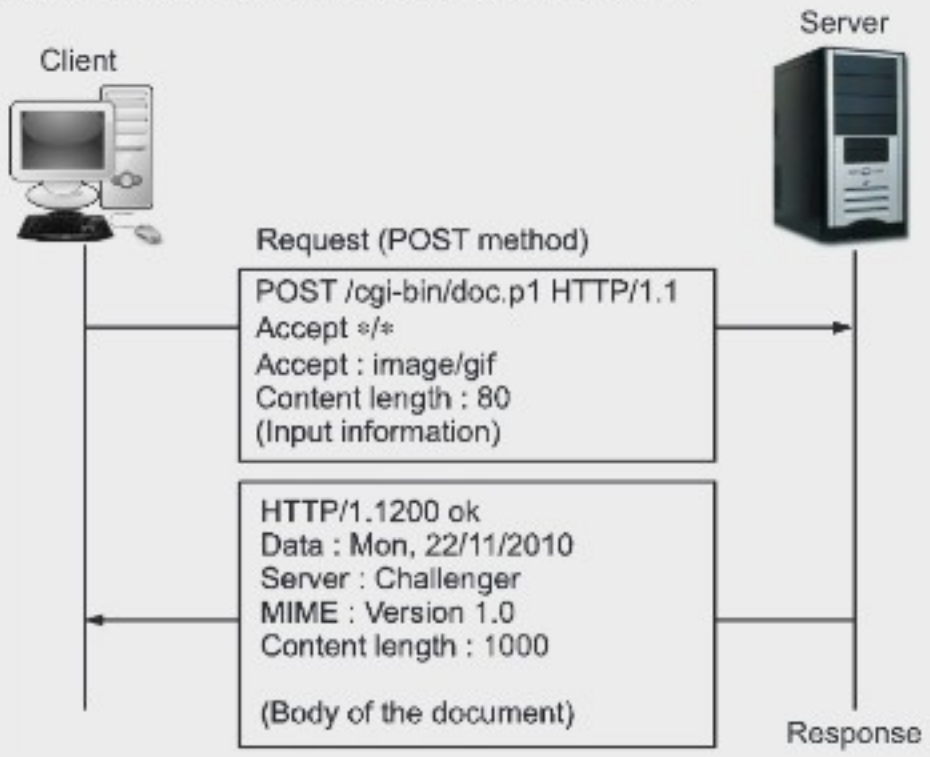


Fig. 6.35: HTTP transaction using POST Method

Summary

- In OSI Model the 4th layer is the Transport Layer. This layer manages end to end (source to destination) (process to process) message delivery in a network.
- The transport layer is responsible for process-to-process delivery - the delivery of a packet, part of a message, from one process to another.
- There are several ways to achieve process to process communication. The most common one is through the client/server paradigm. A process on the local host, called a client, needs services from a process usually on the remote host called a server.
- Process-to-process delivery in the Transport layer needs two identifiers, IP address and port number at both ends to make a connection. The combination of an IP address and a port number is called a socket address.
- Multiplexing and Demultiplexing are the two very important functions that are performed by Transport Layer.
- Transport layer at the sender side receives data from different applications, encapsulates every packet with a transport layer header and passes it on to the underlying network layer. This job of transport layer is known as Multiplexing.
- At the receiver's side, the transport gathers the data, examines its socket and passes the data to the correct Application. This is known as De-multiplexing.
- In a connection oriented service, connection is established first and then data are transferred in between sender and receiver. In a connectionless service, the packets are sent from one machine to another without connection establishment or connection release.
- Transport layer provides reliable as well as unreliable services. If the application layer program needs reliability, transport layer uses a reliable protocol with error control and flow control. If the application program does not need reliability, it may use its own flow and error control or if the service does not demand flow and error control, transport layer uses unreliable UDP protocol.
- The UDP protocol was designed by David P. Reed in 1980 and formally defined in RFC 768. The UDP (User Datagram Protocol) is one of the core members of the Internet protocol suite.
- UDP is a connectionless, unreliable Transport Layer protocol.
- TCP (Transmission Control Protocol) is most widely used protocol for data transmission in communication networks such as the Internet.
- TCP is a reliable and stream oriented protocol.
- Various TCP Services are Process-to-process Communication, Stream Delivery Service, Sending and Receiving Buffers, Segments, Full Duplex Communication, Connection Oriented Service and Reliable Service.
- TCP has several features: Number System, Byte Number, Sequence Number, Acknowledgement Number, Flow Control, Error Control and Congestion Control.
- A packet in TCP is called a segment.

Check Your Understanding

1. Which among the following are delivered by the transport layer in process-to-process delivery mechanism?
   (a) frames (b) datagrams
   (c) packets (d) all of the above
2. What is the purpose of using source and destination port numbers respectively in the addressing method of transport layer?
   (a) for delivery and reply operations
   (b) for reply and delivery operations
   (c) only for delivery operations
   (d) only for reply operations
3. Which mechanism in transport layer supplies multiple network connections along with the distribution of traffic over them in a round-robin basis/ fashion?
   (a) upward multiplexing (b) buffering and flow control
   (c) downward multiplexing (d) crash recovery
4. Transport layer is responsible for process-to-process delivery of the_____
   (a) message (b) address of message
   (c) few packets of message (d) partial message
5. TCP is ..... oriented protocol.
   (a) bit (b) connectionless
   (c) character (d) connection
6. UDP is ..... protocol.
   (a) connectionless (b) connection oriented
   (c) stream oriented (d) both (a) & (b)
7. SCTP is a ..... transport layer protocol.
   (a) reliable (b) connectionless
   (c) connection oriented (d) both (a) & (b)

ANSWER KEY

1. (c)	2. (b)	3. (c)	4. (b)	5. (d)
6. (a)	7. (a)			

Practice Questions

Q.I: Answer the Following Questions in short:

1. What is the transport layer?
2. Which parameter contains by the UDP header?
3. List out different UDP operations.
4. Explain use of UDP in short.
5. List out different TCP services.
6. What is Domain Name System.
7. What is flat and hierarchical namespace .

Q.II: Answer the Following Questions:

1. Explain the process-to-process delivery in detail.
2. Describe the multiplexing and demultiplexing used in transport layer.
3. Explain the connectionless service and connection-oriented service.
4. Explain UDP in detail.
5. Explain the various services of TCP.
6. Describe the features of TCP.
7. Explain the TCP segment format.
8. Explain three sections used in UDP checksum. Which common concepts are used in UDP operation ?
9. "The UDP is called a connectionless, unreliable transport protocol". Justify.
10. Distinguish between reliable and unreliable services.
11. Write short note on
    (i) Domain Namespace
    (ii) E-mail
    (iii) HTTP
    (iv) WWW

Q.III: Define the terms:

1. TCP
2. UDP
3. Process to process delivery
4. node to node delivery
5. multiplexing
6. demultiplexing
7. segment

❖❖❖