

COMPUTER NETWORKS-I

Computer Science (CS-242) : Paper-II

Dr. Ms. MANISHA BHARAMBE
Mrs. VEENA K. GANDHI

CBCS
2 CREDITS



SPPU New Syllabus

A Book Of

COMPUTER NETWORKS-I

For S.Y.B.Sc. Computer Science : Semester – IV (Paper – II)
[Course Code CS 242 : Credits - 2]

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, Associate Professor, Dept. of Comp. Sci.,
MES's Abasaheb Garware College,
Pune

Mrs. Veena K. Gandhi

M.C.S., M.Phil (Comp. Sci.), UGC-NET
Head, Department of B.C.A. (Science),
Abeda Inamdar Senior College,
Pune

Price ₹ 330.00



N5542

COMPUTER NETWORKS-I

ISBN 978-93-90506-39-2

First Edition : January 2021
© **: Authors**

The text of this publication, or any part thereof, should not be reproduced or transmitted in any form or stored in any computer storage system or device for distribution including photocopy, recording, taping or information retrieval system or reproduced on any disc, tape, perforated media or other information storage device etc., without the written permission of Authors with whom the rights are reserved. Breach of this condition is liable for legal action.

Every effort has been made to avoid errors or omissions in this publication. In spite of this, errors may have crept in. Any mistake, error or discrepancy so noted and shall be brought to our notice shall be taken care of in the next edition. It is notified that neither the publisher nor the authors or seller shall be responsible for any damage or loss of action to any one, of any kind, in any manner, therefrom.

Published By :
NIRALI PRAKASHAN

Abhyudaya Pragati, 1312, Shivaji Nagar,
Off J.M. Road, Pune – 411005
Tel - (020) 25512336/37/39, Fax - (020) 25511379
Email : niralipune@pragationline.com

Polyplate

Printed By :
YOGIRAJ PRINTERS AND BINDERS

Survey No. 10/1A, Ghule Industrial Estate
Nanded Gaon Road
Nanded, Pune - 411041
Mobile No. 9404233041/9850046517

➤ DISTRIBUTION CENTRES

PUNE

- Nirali Prakashan :** 119, Budhwar Peth, Jogeshwari Mandir Lane, Pune 411002, Maharashtra
(For orders within Pune)
Tel : (020) 2445 2044; Mobile : 9657703145
Email : niralilocal@pragationline.com
- Nirali Prakashan :** S. No. 28/27, Dhayari, Near Asian College Pune 411041
(For orders outside Pune)
Tel : (020) 24690204; Mobile : 9657703143
Email : bookorder@pragationline.com

MUMBAI

- Nirali Prakashan :** 385, S.V.P. Road, Rasdhara Co-op. Hsg. Society Ltd.,
Girgaum, Mumbai 400004, Maharashtra; Mobile : 9320129587
Tel : (022) 2385 6339 / 2386 9976, Fax : (022) 2386 9976
Email : niralimumbai@pragationline.com

➤ DISTRIBUTION BRANCHES

JALGAON

- Nirali Prakashan :** 34, V. V. Golani Market, Navi Peth, Jalgaon 425001, Maharashtra,
Tel : (0257) 222 0395, Mob : 94234 91860; Email : niralijalgaon@pragationline.com

KOLHAPUR

- Nirali Prakashan :** New Mahadvar Road, Kedar Plaza, 1st Floor Opp. IDBI Bank, Kolhapur 416 012
Maharashtra. Mob : 9850046155; Email : niralikolhapur@pragationline.com

NAGPUR

- Nirali Prakashan :** Above Maratha Mandir, Shop No. 3, First Floor,
Rani Jhansi Square, Sitabuldi, Nagpur 440012, Maharashtra
Tel : (0712) 254 7129; Email : niralinagpur@pragationline.com

DELHI

- Nirali Prakashan :** 4593/15, Basement, Agarwal Lane, Ansari Road, Daryaganj
Near Times of India Building, New Delhi 110002 Mob : 08505972553
Email : niralidelhi@pragationline.com

BENGALURU

- Nirali Prakashan :** Maitri Ground Floor, Jaya Apartments, No. 99, 6th Cross, 6th Main,
Malleswaram, Bengaluru 560003, Karnataka; Mob : 9449043034
Email: niralibangalore@pragationline.com

Other Branches : Hyderabad, Chennai

Note : Every possible effort has been made to avoid errors or omissions in this book. In spite of this, errors may have crept in. Any type of error or mistake so noted, and shall be brought to our notice, shall be taken care of in the next edition. It is notified that neither the publisher, nor the author or book seller shall be responsible for any damage or loss of action to any one of any kind, in any manner, therefrom. The reader must cross check all the facts and contents with original Government notification or publications.

niralipune@pragationline.com | www.pragationline.com

Also find us on  www.facebook.com/niralibooks

Preface ...

We take an opportunity to present this Text Book on "**Computer Networks-I**" to the students of Second Year B. Sc. (Computer Science) Semester-IV as per the New Syllabus, June 2020.

The book has its own unique features. It brings out the subject in a very simple and lucid manner for easy and comprehensive understanding of the basic concepts. The book covers theory of Introduction to Networks and Network Models, Lower Layers, Network Layer and Transport Layer.

A special word of thank to Shri. Dineshbhai Furia, and Mr. Jignesh Furia for showing full faith in us to write this text book. We also thank to Mr. Amar Salunkhe and Mrs. Prachi Sawant of M/s Nirali Prakashan for their excellent co-operation.

We also thank Mr. Ravindra Walodare, Mr. Sachin Shinde, Mr. Ashok Bodke, Mr. Moshin Sayyed and Mr. Nitin Thorat.

Although every care has been taken to check mistakes and misprints, any errors, omission and suggestions from teachers and students for the improvement of this text book shall be most welcome.

Authors

Syllabus ...

1. Introduction to Networks and Network Models (4 Hrs.)

- 1.1 Data Communication, Components, Data Representation
- 1.2 Networks, Network Criteria, Network Types - LAN, WAN, Switching, The Internet, Accessing the Internet
- 1.3 Network Software - Protocol Hierarchies, Design Issues of the Layer, Connection Oriented and Connectionless Services
- 1.4 Reference Models - OSI Reference Models, TCP/IP Reference Model, Connection Devices in different Layers, Comparison of OSI and TCP/IP Reference Models

2. Lower Layers (10 Hrs.)

- 2.1 Communication at the Physical Layer, Data Rate Limits - Noiseless Channel (Nyquist Bit Rate), Noisy Channel (Shannon Capacity), Performance - Bandwidth, Throughput, Latency, Bandwidth-Delay Product, Jitter
- 2.2 Design Issues of Data Link Layer, Services - Framing, Flow Control, Error Control, Congestion Control, Link Layer Addressing
- 2.3 Framing Methods - Character Count, Flag Bytes with Byte Stuffing, Flags Bits with Bit Stuffing, Physical Layer Coding Violations
- 2.4 The Channel Allocation Problem, Static and Dynamic Allocation, Media Access Methods - Taxonomy of Multiple - Access Protocols
- 2.5 Switching and TCP/IP Layers, Types - Circuit Switching, Packet Switching and Message Switching
- 2.6 Wired LANs - Standard Ethernet Characteristics, Addressing, Access Method, Implementation, Fast and Gigabit Ethernet
- 2.7 Wireless LANs - Architectural Comparison, Characteristics, Access Control, IEEE 802.11 Architecture, Physical Layer, MAC Sublayer, Bluetooth Architecture, Layers

3. Network Layer (12 Hrs.)

- 3.1 Network Layer Services - Packetizing, Routing and Forwarding, other Services
- 3.2 Open and Closed Loop Congestion Control
- 3.3 IPv4 Addressing - Address Space, Classful Addressing, Subnetting, Supernetting, Classless Addressing, Network Address Resolution (NAT)
- 3.4 Forwarding of IP Packets - Based on Destination Address, Based on Label
- 3.5 Network Layer Protocols - Internet Protocol (IP), IPv4 Datagram Format, Fragmentation, Options
- 3.6 Mobile IP - Addressing, Agents, Three Phases
- 3.7 Next Generation IP - IPv6 Address Representation, Address Space, Address Types, IPv6 Protocol, Packet Format, Extension Header, Difference between IPv4 and IPv6
- 3.8 Routing - General Idea, Algorithms - Distance Vector Routing, Link State Routing, Path - Vector Routing

4. Transport Layer **(10 Hrs.)**

- 4.1 Transport Layer Services - Process-to-Process Communication, Addressing, Encapsulation and Decapsulation, Multiplexing and Demultiplexing, Flow Control, Pushing or Pulling, Sequence Numbers, Acknowledgements, Sliding Window, Congestion Control
- 4.2 Connectionless and Connection-oriented Service, Port Numbers
- 4.3 Transport Layer Protocols - User Datagram Protocol, User Datagram, UDP Services
- 4.4 Transmission Control Protocol - TCP Services, TCP Features, TCP Segment Format, Three-way Handshake for Connection Establishment and Termination, State Transition Diagram, Windows in TCP



Contents ...

1. Introduction to Networks and Network Models	1.1 – 1.82
2. Lower Layers	2.1 – 2.98
3. Network Layer	3.1 – 3.90
4. Transport Layer	4.1 – 4.48



Introduction to Networks and Network Models

Objectives...

- To understand Concepts in Data Communication
- To learn Network and Computer Network
- To study Basic Concepts of Internet
- To learn Network Software
- To study Reference Models (OSI and TCP/IP)

1.0 INTRODUCTION

- Data communications and computer networks are two of the fastest growing technological areas in today's modern world. This is because there is an almost unlimited demand for information transfer.
- The word 'communication' is derived from the Latin word 'communicare', which means 'to share'. Communication means the transfer of information between humans, computers or machines in a meaningful way.
- Communication is the process of establishing connection or link between two entities for the transfer/exchange of information.
- 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.
- Data communication is a process of exchanging data or information between two devices (a sender and a receiver) through some kind of transmission/ communication medium such as coaxial cable or fiber optic cable (wired) and/or air (wireless).
- A group of computers and other devices such as printers, hubs, modems etc., connected together is called a network. The interconnected computers can share resources, which is called networking.
- A computer network provides the facility of information exchange/transfer among the computers, connected to it.

- A network is a combination of hardware and software that sends data from one point 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, that make possible the services that we expect from a network.
- A reference model in networking is a conceptual layout that describes how communication between devices should occur.
- For efficient communication, the reference model identifies the tasks involved in inter-computer communication and divides them in logical groups called layers, with each layer performing a specific function.
- The purpose of the reference model was to define an architectural framework that defines the logical communication tasks that are required to move information between different computer systems.
- In networking the two most common reference models are Open Systems Interconnection (OSI) reference model and TCP/IP (Transmission Control Protocol/Internet Protocol) reference model.
- In this chapter we will study basic concepts in data communications and networking, reference models, network software, Internet and so on.

1.1 DATA COMMUNICATION

- Today, technologies related to data communications and networking may be the fastest growing in our culture and/or our modern society.
- The appearance of new social networking applications like Facebook, Twitter etc., every year is a testimony to this claim.
- People use the Internet more and more every day and they use the Internet for research, banking, shopping, ticket booking (bus, airplane, railway etc.), weather, education and so on.
- Communication is the basic process of information exchange. Communication, whether between human beings or computer systems, involves transfer of information from a sender to a receiver.
- Communication is the conveyance of a message from one entity, called the source or transmitter or sender to another entity called the destination or receiver, using a communication channel/medium.
- Communication is defined as, transfer of information such as thoughts and messages between two entities. The process of sending or receiving data between two points/entities of a computer network is known as data communication.

- Data communication is the exchange of information between two computers capable of generating processing and interpreting data.
- The data communication process shown in Fig. 1.1.

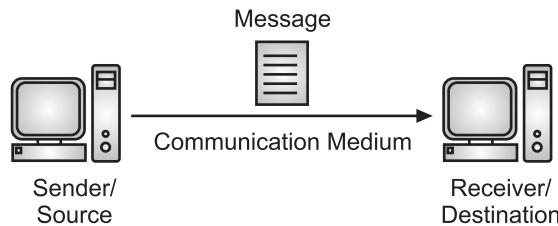


Fig. 1.1: Communication between Two Computers

- Fig. 1.1 shows communication between one computer (sender/source) sending a message to another computer (receiver/destination) over a wire or radio waves called transmission media.
- The data plays an important role in networking. Data is defined as ‘raw facts and figures before they have been processed’.
- The meaningful, logical and processed data is called information. Information can be defined as ‘meaningful data or processed data’.

Comparison between Data and Information:

Sr. No.	Data	Information
1.	Data is a collection of raw facts and figures.	Information is processed data.
2.	Data is unarranged and unorganized.	Information is arranged and organized
3.	Data is a raw (meaningless) facts that required to be processed to make it meaningful.	Information is meaningful.
4.	Data is input.	Information is output.
5.	Data is raw material for information.	Information is the final product of data.
6.	Data depends upon the sources.	Information depends upon data.

- Data communication refers to the exchange of data between a source and a receiver via some form of transmission medium.
- The effectiveness of a data communication systems depends on four fundamental characteristics as given below:
 1. **Delivery:** The system must deliver data to the correct destination. Data must be received by the intended device or user.

2. **Accuracy:** The system must deliver the data accurately i.e., without any error.
3. **Timeliness:** The system must deliver data in a timely manner. Data delivered late is useless.
4. **Jitter:** Jitter refers to the variation in the packet arrival time. Jitter is the uneven delay in the delivery of audio or video packets.

1.1.1 Definition of Data Communication

- The term data communication can be defined as “the process of using computing and communication technologies to transfer data from one place to another, and vice versa”. **OR**
- Data communication refers to the exchange of data between a source and a receiver via form of transmission media such as a wire cable (twisted-pair cable or coaxial cable) or wireless (air). **OR**
- “The transfer or exchange of information from one computer to another is known as data communication”.

1.1.2 Components of Data Communication

- The purpose of data communications is to provide the rules and regulations that allow computers with different disk operating systems, languages, cabling and locations to share resources.
- Data communication refers to the exchange of information/data between two devices through some form of wired or wireless transmission medium.
- Data communication includes the transfer of data, the method of transfer and the preservation of the data during the transfer/exchange process.
- To initiate data communication, the communicating devices should be a part of a data communication system that is formed by the collection of physical equipment's (hardware) and programs (software).
- A data communication system has five components namely sender, message, receiver, transmission medium, and protocol are shown in Fig. 1.2.

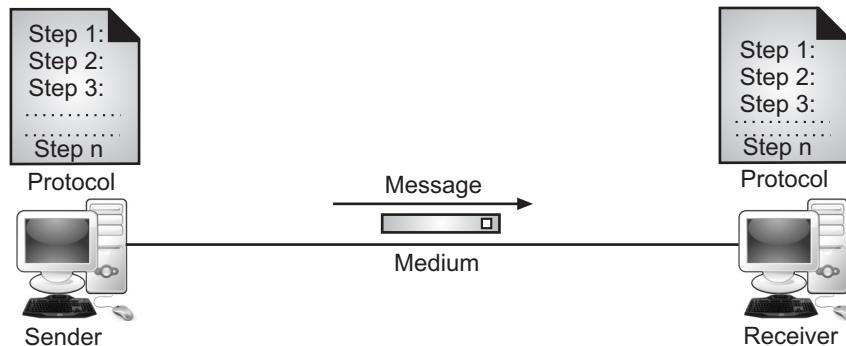


Fig. 1.2: Components of Data Communications

- Fig. 1.2 shows the following components of data communication:
 1. **Sender:** The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, and so on.
 2. **Message:** The message is the information (data) to be communicated. It can consist of text, pictures, sound, or video- or any combination of these.
 3. **Medium:** The transmission medium is the physical path by which a message travels from sender to receiver. It could be a twisted-pair wire, coaxial cable, fiber-optic cable, or radio waves.
 4. **Protocol:** A protocol is a set of rules that governs data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but could not communicate.

A protocol refers to a set of rules (agreed upon by the sender and the receiver) that coordinates the exchange of information. A protocol is a set of rules that governs data communication. Protocol is very important for networking without protocol communication cannot occur. A protocol is defined as, "a formal set of rules, conventions and data structure that governs how computers and other network devices exchange information over a network."

A protocol defines basic elements namely, Syntax (what is to be communicated?) Semantics (how it is to be communicated?) and Timing (when it should be communicated?).

(April 17, Oct. 18)

- 5. **Receiver:** The receiver is the device that receives the message. It can be computer, workstation, telephone handset, television, and so on.

1.1.3 Data Representation

- Data representation refers to the methods used internally to represent information stored in a computer.
- Information today comes in various forms like text, numbers, images, audio, and video.
 1. **Text:** In data communication, text is represented as a bit pattern, a sequence of 0s or 1s. Different sets of bit patterns have been designed to represent text symbols. The process of representing symbols is called coding. Today, Unicode (32 bits) and American Standard Code for Information Interchange [(ASCII) specifies character values from 0 to 127] used to represent a symbol or character used in any language in the world.
 2. **Numbers:** Numbers are also represented by bit patterns. ASCII is not used to represent numbers. the number is directly converted into binary to simplify mathematical operations.

3. **Images:** Images are also represented by bit patterns. An image is composed of a matrix of pixels (picture elements). Each pixel in an image is a small dot and each pixel is assigned a bit pattern whose size depends on the nature of the image. To represent a color image, a method like RGB and YCM are used. RGB method uses primary colors Red, Green, and Blue to make every color. YCM method uses colors Yellow, Cyan, and Magenta to make every color.
4. **Audio:** Audio refers to the recording or broadcasting of sound or music. It is continuous, not discrete. The sound is recorded with a microphone and then digitized to represent in the form of bit-patterns.
5. **Video:** Video refers to the recording or broadcasting of a picture or movie. Video can either be produced as a continuous entity by a TV camera or video can be a combination of images, each discrete entity, arranged to convey the idea of motion.

1.1.4 Data Flow

(Oct. 17)

- The direction of data flow between two linked devices is called as mode of communication.
- There are three types of direction of data flow namely, simplex communication mode, half-duplex communication mode and full-duplex communication mode.

1. Simplex Communication Mode:

- In simplex mode, the communication can take place in only one direction.
- In simplex mode, a terminal can only send data and cannot receive it or it can only receive data but cannot send it. It means that in simplex mode communication is unidirectional.
- Fig. 1.3 shows simplex mode in data communication.

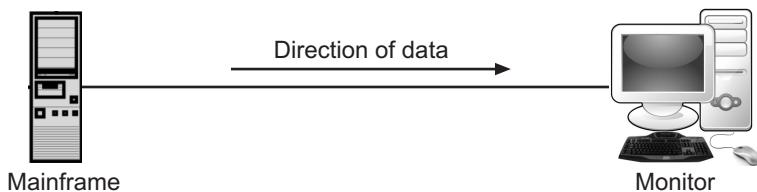


Fig. 1.3: Simplex Communication Mode

- In computer systems, the keyboard, monitor and printer are examples of simplex communication. The keyboard can only be used to enter data into the computer, while monitor and printer can only accept (display/print) output.

Advantages of Simplex Communication Mode:

- (i) Very simple and easy communication method.

- (ii) Cheaper in cost.

Disadvantages Simplex Communication Mode:

- (i) Only allows for communication in one direction.
- (ii) Simplex transmission is not often used because it is not possible to send back error to the transmit end.

2. Half-Duplex Communication Mode:

- In half-duplex mode, the communication can take place in both directions, but only in one direction at a time.
- In this mode, data is sent and received alternatively. It is like a one-lane bridge where two-way traffic must give way in order to cross the other.
- In simple words, in half duplex mode, at a time only one end transmits data while the other end receives.
- A walkie-talkie operates in half duplex mode. It can only send or receive a transmission at any given time. It cannot do both at the same time.
- Fig. 1.4 shows half-duplex communication mode.

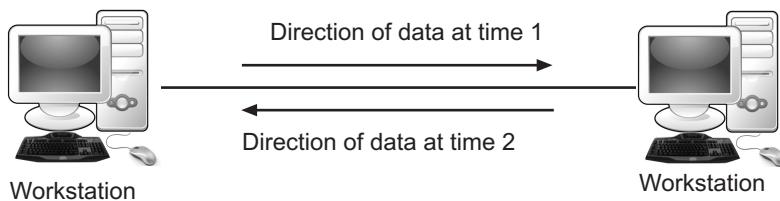


Fig. 1.4: Half-duplex Communication Mode

Advantages Half Duplex Communication Mode:

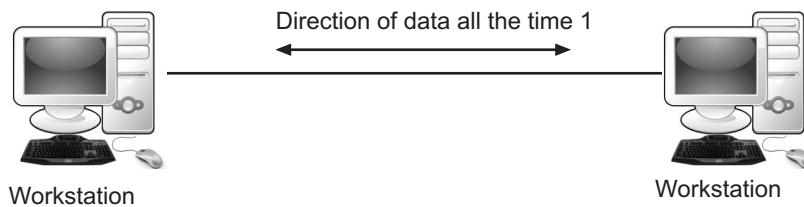
- (i) Enable two-way communication.
- (ii) Low cost than full duplex communication mode.

Disadvantages Half Duplex Communication Mode:

- (i) Only one device can transmit at a time.
- (ii) Higher cost than simplex mode.

3. Full-Duplex Communication Mode:

- In full-duplex mode, the communication can take place in both directions simultaneously, i.e. at the same time on the same channel.
- For example, the telephone communication system is an example of full-duplex communication mode.
- Fig. 1.5 shows full-duplex communication mode.

**Fig. 1.5: Full Duplex Communication Mode****Advantages:**

- (i) Enables two-way communication simultaneously.
- (ii) Fastest method of data communication.

Disadvantages:

- (i) More expensive and complex method.
- (ii) Two bandwidth channels are required for data transmission.

1.2 NETWORKS

- A network is the interconnection of a set of devices (like a host (desktop, laptop, workstation, smartphone) and/or connecting devices like router, switch, modem etc.).
- A network is nothing more than two or more computers connected by a cable or by a wireless radio waves connection so that they can exchange information.
- A communication network is a set of devices connected by channels on links and provides a service between users located at various geographical points.
- A network is defined as, “an interconnected collection of autonomous computers”. Two computers are said to be interconnected if they are capable of exchanging information.

1.2.1 Computer Networks

(April 17, 19)

- A computer network is an interconnection of computers and computing devices using either wires or radio waves over small or large geographical areas.
- A computer network refers to a collection of two or more computers (nodes) which are connected together to share information and resources.
- 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) connected by communication media links (See Fig. 1.6).
- A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.
- The links connecting the devices are often called communication channels. The term channel refers to a communication path between two communicating devices.

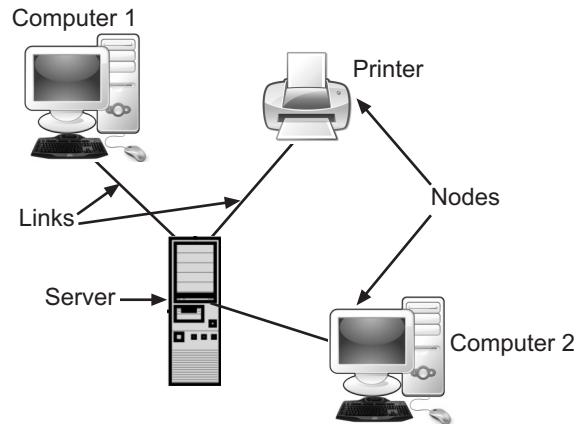


Fig. 1.6: Network Nodes and Links

- 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.
- In simple words, a computer network is a group of interconnected computing devices. The interconnected computers can share resources, which is called networking.
- Computer network is divided into wired and wireless networks. Fig. 1.7 shows diagrammatic representation of computer networks (wired and wireless).

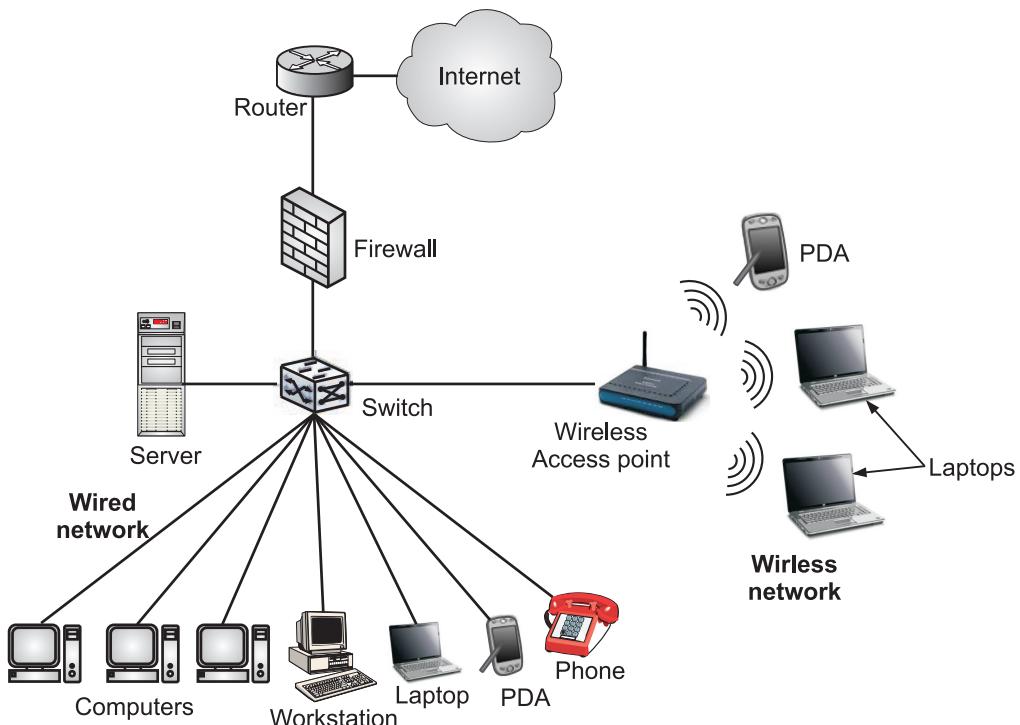


Fig. 1.7: Computer Network (Wired and Wireless)

- A **wired network** is simply, a collection of nodes connected by cables like Ethernet, coaxial, fiber optic cable etc. A **wireless network**, which uses high-frequency radio waves to communicate between nodes.
- The following **characteristics** should be considered in computer network design and ongoing maintenance:
 1. **Availability:** Availability is typically measured in a percentage based on the number of minutes that exist in a year. Therefore, uptime would be the number of minutes the network is available divided by the number of minutes in a year.
 2. **Cost:** Includes the cost of the network components, their installation, and their ongoing maintenance.
 3. **Reliability:** Defines the reliability of the network components and the connectivity between them. Mean Time Between Failures (MTBF) is commonly used to measure reliability.
 4. **Security:** Includes the protection of the network components and the data they contain and/or the data transmitted between them.
 5. **Speed:** Includes how fast data is transmitted between network endpoints, (the data rate).
 6. **Scalability:** Defines how well the network can adapt to new growth, including new users, applications, and network components.
 7. **Topology:** Describes the physical cabling layout and the logical way data moves between components.
 8. **Integration:** All the components of the network work in a coordinated manner for a seamless user experience.
 9. **Sharing:** Computer networks enable sharing of files, software, hardware resources and computing capabilities.

1.2.2 Definition of Computer Network

- The old model of a single computer serving all of the organization's computational needs has been replaced by one in which a large number of separate but interconnected computers do the job. These systems are called computer networks.
- A computer network, often simply referred to as a network, is a collection of computers and computing devices connected by communication channels that facilitate communication among users and allow shared resources.
- A computer network provides the facility of information exchange/transfer among the computers, connected to it.
- Computer networking is a very important and crucial part of Information Technology (IT). Millions of computers are networked together to form the Internet.

- Networking plays an important role in every kind of organization from small to medium sized, in banks, multinational companies, stock exchanges, airports, hospitals, police stations, post offices, colleges, universities and even in the home. In short networking plays an important role everywhere where computers are used.
- 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 equipment like printer, scanner etc. using either wires or radio waves (wireless) made to share hardware and software resources".
- Fig. 1.8 shows a typical computer network.

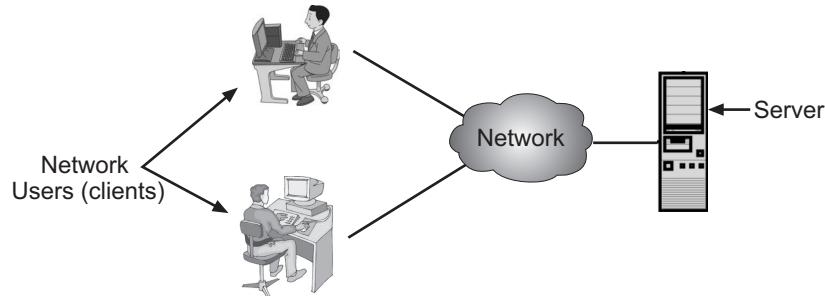


Fig. 1.8: Typical Computer Network

- 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. The major networking services are:
 - File Services:** This includes file transfer, storage, data migration, file update, synchronization and achieving.
 - Printing Services:** This service provides shared access to valuable printing devices.
 - Message Services:** This service facilitates email, voice mails and coordinate object oriented applications.
 - Application Services:** This services allows us to centralize high profile applications to increase performance and scalability.
 - Database Services:** This involves coordination of distributed data and replication.

1.2.3 Network Criteria

- To be considered effective and efficient, a computer network must meet a number of criteria. The most important of computer network criteria are performance, security and reliability.

1. Performance:

- Performance of computer networks can be measured in many ways, including transit time (propagation delay) and response time (speed of operation).
- Transit time is the amount of time required for a message to travel from one device to another in a network. Response time in the network is the elapsed time between an inquiry and a response.
- The performance of a network depends on a number of factors. Some of them are explained below:

(i) Type of Transmission Medium:

- The transmission medium defines the speed at which data can travel through a connection (the data rate). Today's networks are moving to faster and faster transmission media, such as fiber-optic cabling.
- A transmission medium that can carry data at 100 megabits per second is 10 times more powerful than a medium that can carry data at only 10 megabits per second.

(ii) Number of Users:

- Having a large number of concurrent users can slow response time in a computer network not designed to coordinate heavy traffic loads.
- The design of a given computer network is based on an assessment of the average number of users that will be communicating at any one time.
- When the actual number of users can exceed the average and thereby decrease performance. How a network responds to loading is a measure of its performance?

(iii) Software:

- The software used to process data at the sender, receiver, and intermediate nodes also affects network performance.
- Moving a message from node to node through a network requires processing to transform the raw data into transmittable signals, to route these signals to the proper destination, to ensure error-free delivery, and to recast the signals into a form the receiver can use.
- The software that provides these services affects both the speed and the reliability of a network link. A well designed software can speed the process and make data transmission more effective and efficient.

(iv) Hardware:

- The types of hardware included in a computer network affect both the speed and capacity of data transmission. A higher-speed computer with greater storage capacity provides better performance.

2. Security:

- Network security issues in a computer network include protecting data from unauthorized access and viruses.

(i) Unauthorized Access:

- For a computer network to be useful, sensitive data must be protected from unauthorized access. Protection can be accomplished at a number of levels.
- At the lowest level are user identification codes and passwords while at a higher level are encryption techniques.
- In these mechanisms, data are systematically altered/modified in such a way that if they are intercepted by an unauthorized user, they will be unintelligible.

(ii) Viruses:

- A computer network is accessible from many points, it can be susceptible to computer viruses. A virus is an illicitly introduced code that damages the computer system.
- A good computer network is protected from viruses by hardware and software designed specifically for that purpose.

3. Reliability:

- In addition to accuracy of delivery, network reliability of a computer network is measured by following factors:

(i) Frequency of Failure:

- All networks fail occasionally. A network that fails often, however, is of little value to a user.

(ii) Recovery Time of a Network After a Failure:

- How long does it take to restore service? A computer network that recovers quickly is more useful than one that does not.

(iii) Catastrophe:

- Computer networks must be protected from catastrophic events such as fire, earthquake or theft.
- One protection against unforeseen damage is a reliable system to back up computer network software.

1.2.4 Physical Structures

- Before studying computer networks, we need to define some network attributes like type of connection and physical topology.

1.2.4.1 Type of Connection

- In order to communicate to each other, two or more devices in a computer network, must be connected using a link.
- A link is a communications pathway that transfers data from one device to another. For communication to occur, two devices must be connected in some way to the same link at the same time.
- The two types of connections are point-to-point and multipoint. Both types of connections describe a method to connect two or more communication devices in a link.

1. Point-to-Point Connection:

(April 16)

- Connection between two directly interconnected devices/nodes is referred to as point-to-point connection.
- A point-to-point connection provides a dedicated link between the two devices/nodes as shown in Fig. 1.9. The entire capacity of the link is used for the transmission between those two devices.
- The point-to-point connection is a unicast connection. There is a dedicated link between an individual pair of sender and receiver.
- A point-to-point connection is a direct link between two devices/nodes such as a workstation and a workstation (See Fig. 1.9).
- For example, when we change television channels by using remote control, we establish a point-to-point connection between the remote control and television.

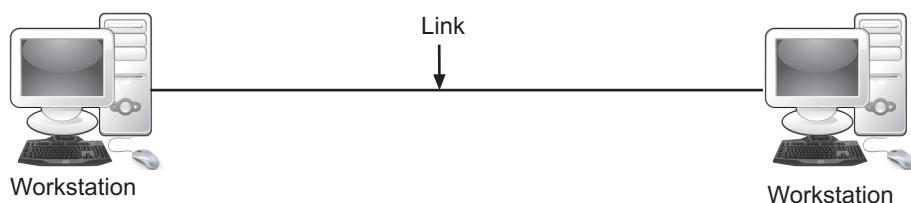


Fig. 1.9: Point-to-point Connection

2. Multipoint Connection:

- A multipoint connection is a link between more than two devices. It is also known as multidrop connection.
- In multipoint connection, a single link is shared by multiple devices. So, it can be said that the channel capacity is shared temporarily by every device connecting to the link.
- The networks having multipoint connections are called broadcast networks. A broadcast network has a single communication channel that is shared by all the machines on the network.
- Examples of multipoint connections are Ethernet and Bus topology based on LAN.

- Fig. 1.10 shows a broadcast network. In Fig. 1.10 we can see that the three workstations share the common link between the mainframe and the workstations.

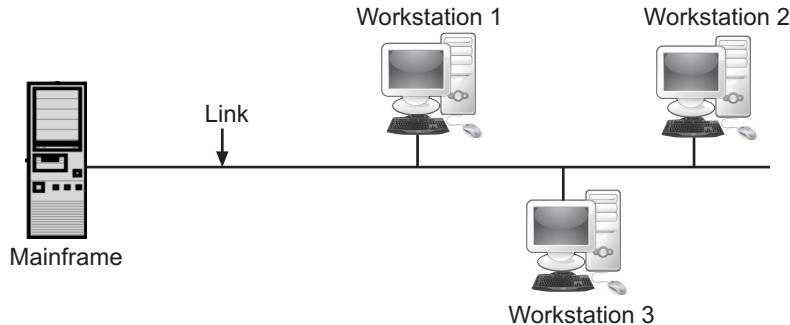


Fig. 1.10: Broadcast Connection

- In a multipoint connection environment, the capacity of channel is shared, either spatially or temporally.
- If several devices can share the link simultaneously, it is called spatially shared connection. If users must take turns using the link, then it is called temporally shared or time shared connection.

1.2.4.2 Physical Topology

- The word “topology” comes from “topos”, which is Greek word for “place.” The term physical topology refers to the way in which a network is laid out physically.
- Network topology refers to the layout of a network and how different nodes in a network are connected to each other and how they communicate.
- The topology of a network is defined as “the geometric representation of the relationship of all the links and linking devices (nodes) in a network”.
- A physical topology describes the placement of network nodes and the physical connections between them.
- The physical topology of a network refers to the configuration of cables, computers, and other peripherals.
- Bus topology, star topology, ring topology, tree topology, mesh topology, etc. are the examples of physical topologies.

1.2.4.2.1 Star Topology

(April 17, 18, 19, Oct. 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 a central controller (Hub/Switch) only. Star topology is generally used in LANs.
- Fig. 1.11 shows a star topology or network.

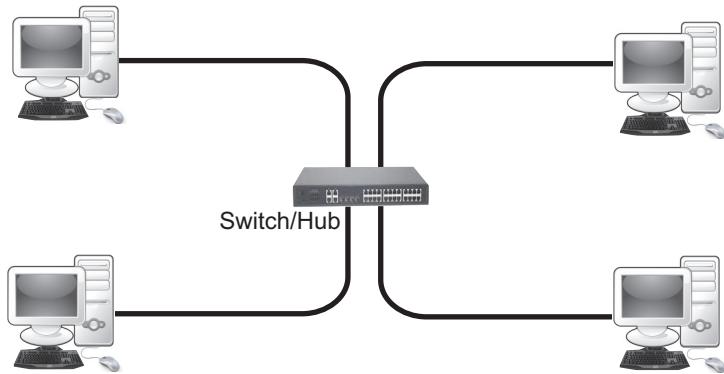


Fig. 1.11: Star Topology

Advantages:

1. Easy to install, reconfigure and wire.
2. Centralized management which helps in monitoring the network.
3. Fast as compared to ring topology.
4. Multiple devices can transfer data without collision.
5. Eliminates traffic problems.
6. No disruptions to the network when connecting or removing devices.
7. It is easy to detect the failure and troubleshoot it.

Disadvantages:

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

1.2.4.2.2 Bus Topology

(April 16)

- In bus topology, all nodes are connected to a central cable which is called a bus. This bus is also called Trunk or sometimes it was also referred to as Backbone cable.
- Trunk cable was 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 up the wire, all the computers on the network receive the information, but only one accepts the information.
- The rest rejects 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.

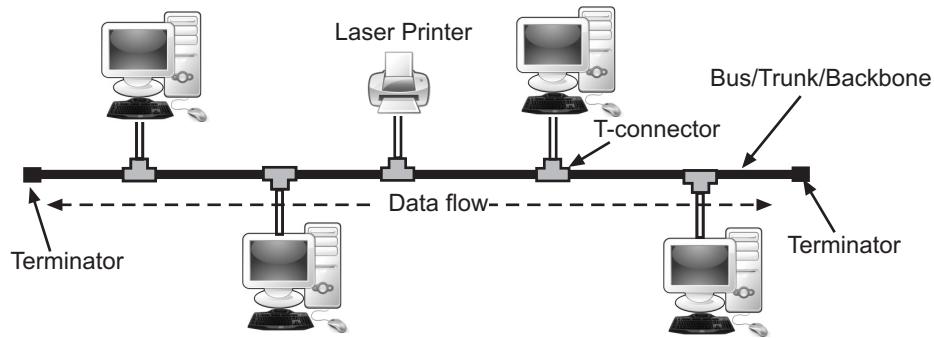


Fig. 1.12: Bus Topology

Advantages:

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

Disadvantages:

1. It cannot 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 a small network.

1.2.4.2.3 Ring Topology

(April 18, Oct. 17)

- 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 a 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 flows around the ring in one direction. Today higher speed LANs has made this topology less popular.
- Fig. 1.13 shows a ring topology.

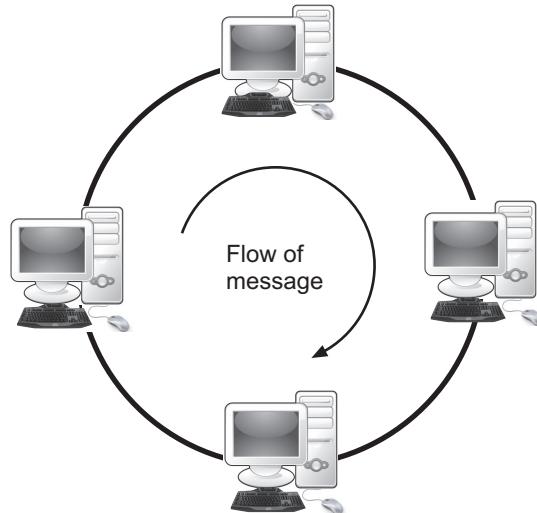


Fig. 1.13: Ring Topology

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. Its performance is better than that of Bus topology.
7. 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 nodes, the whole network must be down first.
4. Traffic is unidirectional.

Comparison between Bus, Ring and Star Topologies:

Terms	Bus Topology	Ring Topology	Star Topology
Structure	There is a single central cable (backbone) and all computers and other devices connect to it.	All computers and other devices are connected in a circle or ring.	There is a central host (hub/switch) and all nodes connect to it.

Contd...

Host existence	Depends on network needs.	Depends on network needs.	Yes.
Connection between nodes	It has no connection between the nodes.	Yes.	No.
Host failure	Network can still run.	Network will fail.	Network will fail.
Trouble-shooting	Difficult, there is a need to search for the problematic node one by one.	Depends on backbone. If there is backbone, trouble-shooting is difficult. If there is no 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.
Ease of adding or removing nodes	Easy.	Difficult.	Average.
Number of nodes when extending network	Many.	Limited.	Limited.

1.2.4.2.4 Mesh Topology

(April 16, 17, 18, 19)

- In a mesh network topology, each of the network nodes, computer and other devices, are interconnected with one another with dedicated point to point link.
- Dedicated means that a link carries traffic only between the two devices it connects. So for N number of nodes, there will be a total $n(n-1)/2$ links required.
- 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. 1.14 shows a mesh topology. Mesh topology is used in WAN.

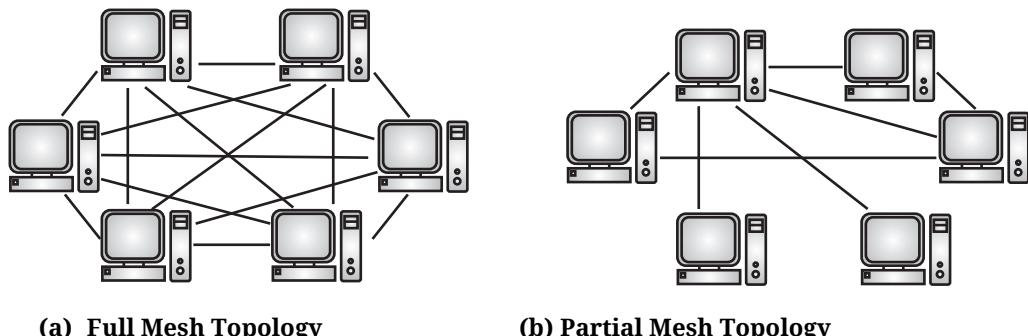


Fig. 1.14: Mesh Topology

- A mesh topology employs one of two connection arrangements, full mesh topology or partial mesh topology.
 1. In a **full mesh network**, each network node is connected to every other node in the network. Due to this arrangement of nodes, it becomes possible for a simultaneous transmission of signals from one node to several other nodes.
 2. In a **partially connected mesh network**, only some of the network nodes are connected to more than one node. This is beneficial over a fully connected mesh in terms of redundancy caused by the point-to-point links between all the nodes.

Advantages:

1. Each connection can carry its own data load due to a dedicated link.
2. Eliminates traffic problems.
3. Mesh topology is robust. If one link becomes unusable, it does not affect other systems.
4. Privacy or security because of dedicated lines.
5. Point-to-point links 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. Set-up and maintenance of this topology is very difficult.
5. Expensive due to hardware requirements such as cables.

1.2.4.2.5 Tree Topology

- As its name implies in this topology devices make a tree structure. It is also called a hierarchical topology.
- Tree topology integrates the characteristics of star and bus topology. In tree topology, the numbers of star networks are connected using Bus.
- This main cable seems like a main stem of a tree, and other star networks as the branches.
- Ethernet protocol is commonly used in this type of topology. Fig. 1.15 shows tree topology.

Advantages:

1. Easy to install and wire.
2. Fast as compared to other topologies.
3. Multiple devices can transfer data without collision.
4. It eliminates traffic problems.

5. No disruptions to the network then connecting or removing devices.
6. Easy to detect faults and to remove parts.

Disadvantages:

1. It relies heavily on the main bus cable, if it breaks the whole network is crippled.
2. More expensive than other topologies.
3. The cabling cost is more.
4. Scalability of the network depends on the type of cable used.
5. As more and more nodes and segments are added; the maintenance becomes difficult.

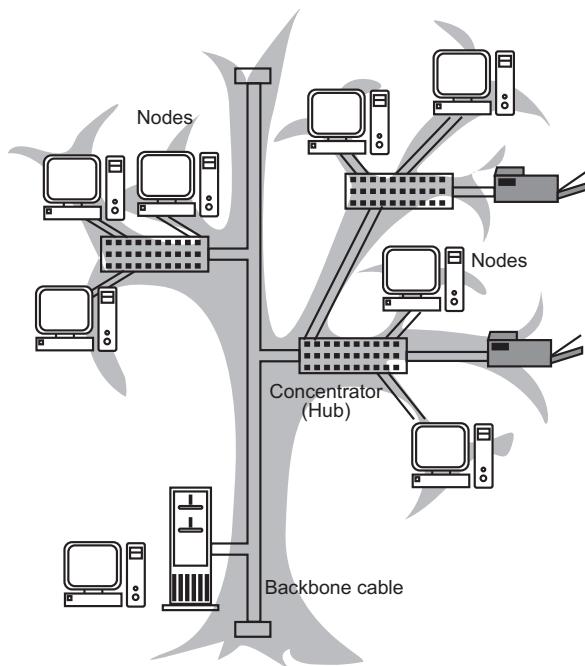


Fig. 1.15: Tree Topology

1.2.4.2.6 Hybrid Topology

- Hybrid, as the name suggests, is a mixture of two different things. A hybrid topology is a combination of two or more network topologies.
- The topology that combines more than one topology is called hybrid topology.
- Two common examples for hybrid networks are star ring network and star bus network.
 1. **A star-ring network** consists of two or more star topologies connected using a Multistation Access Unit (MAU) as a centralized hub.
 2. **A star-bus network** consists of two or more star topologies connected using a bus trunk (the bus trunk serves as the network's backbone).

- Fig. 1.16 shows an example of star-bus hybrid topology.

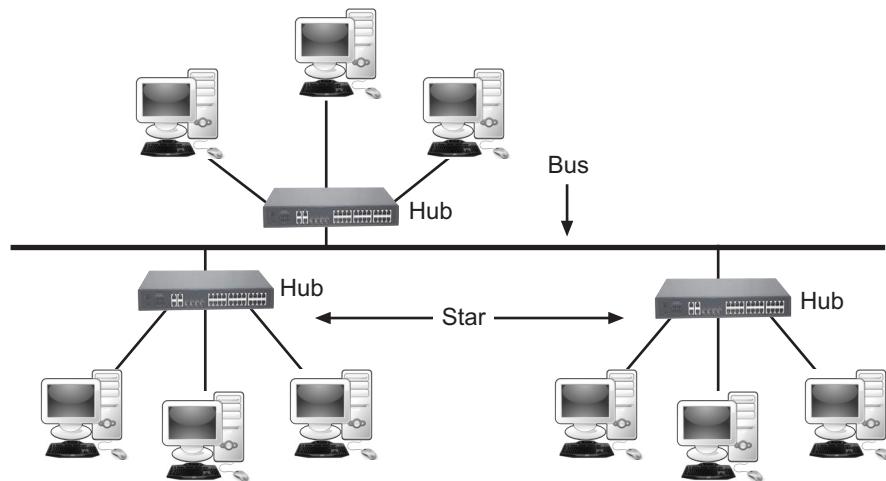


Fig. 1.16: Hybrid Topology

Advantages:

- Fault detection and troubleshooting is easy in this type of topology.
- It is easy to increase the size of a network by adding new components, without disturbing existing architecture.
- Flexible because this topology can be designed according to the requirements of the organization and by optimizing the available resources.
- Hybrid topology is the combination of two or more topologies, so we can design it in such a way that strengths of constituent topologies are maximized while their weaknesses are neutralized.

Disadvantages:

- Hybrid topology is complex and difficult to design.
- The hubs used to connect two distinct networks are very expensive.
- As hybrid architectures are usually larger in scale, and so it is time consuming and difficult to install.
- Hybrid topology also requires a lot of cables, cooling systems, sophisticated network devices, etc.
- Cost is high.

1.2.5 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. 1.17.

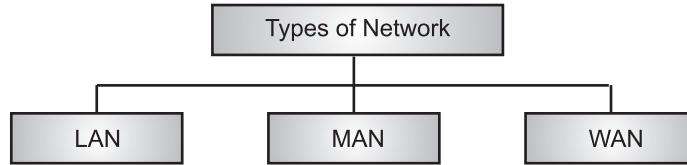


Fig. 1.17: Types of Computer Network

- Fig. 1.18 shows geographical arrangement of LAN, WAN and MAN.

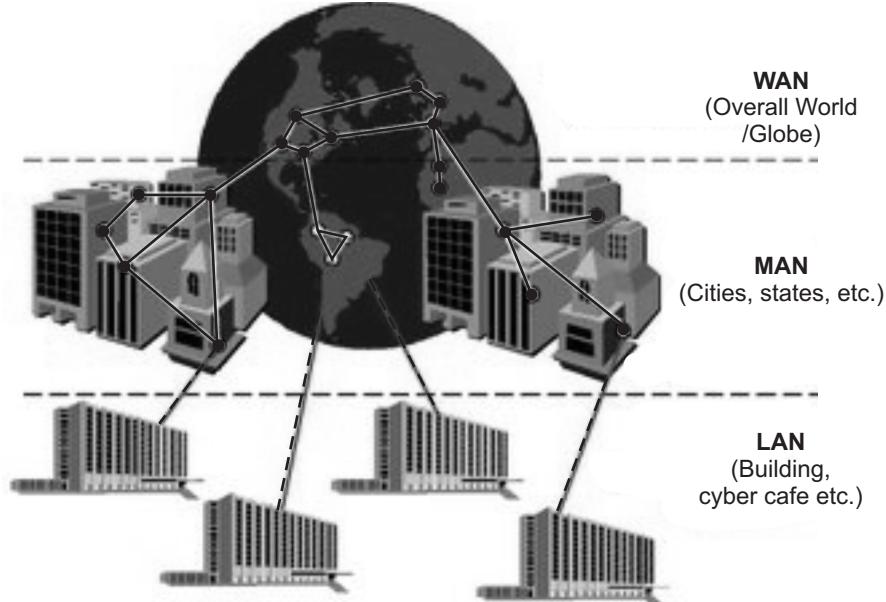
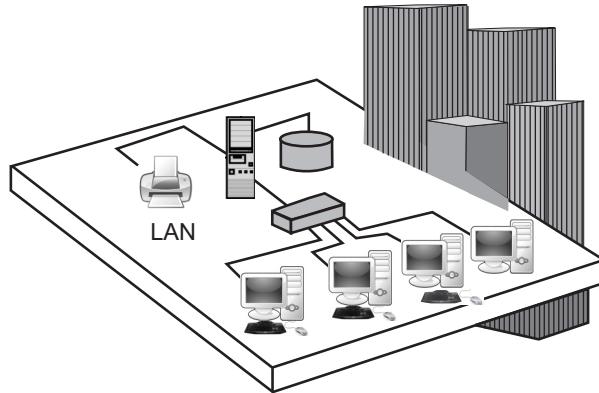


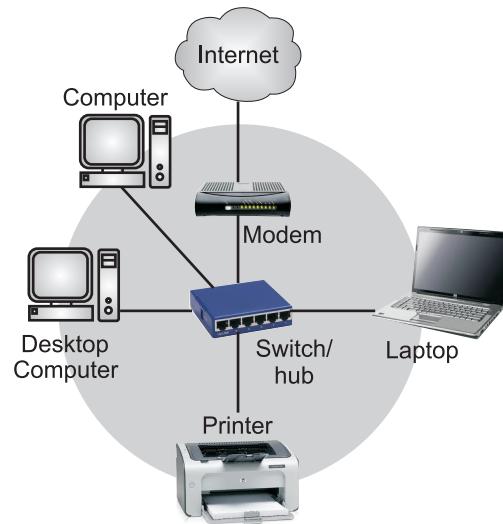
Fig. 1.18: Geographical Arrangement of LAN, WAN and MAN

1.2.5.1 Local Area Network (LAN)

- Local Area Networks (LANs) 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 an organization.
- LANs are widely used to connect personal computers and workstations to share resources (printers, scanners) and exchange information.
- In LAN computers housed locally within a building or a campus and interlinked by a single shared medium like cable (See Fig. 1.19).
- LANs are designed to allow resources to be shared between personal computers or workstations. The resources to be shared can include hardware (e.g., a printer), software (e.g., an application program) or data.
- LANs are distinguished from other kinds of networks by three characteristics i.e., their size, their transmission technology and their topology.

**Fig. 1.19: A Typical Building LAN**

- 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.
- A LAN may be set up using wired or wireless connections. A LAN that is completely wireless is called Wireless LAN (WLAN).
- WLAN helps us to link single or multiple devices using wireless communication within a limited area like home, school, or office building. Today most modern day's WLAN systems are based on IEEE 802.11 standards.
- On most LANs, cables are used to connect nodes like computers, printers, etc. Fig. 1.20 shows a typical LAN.

**Fig. 1.20: A Typical LAN**

Advantages of LAN:

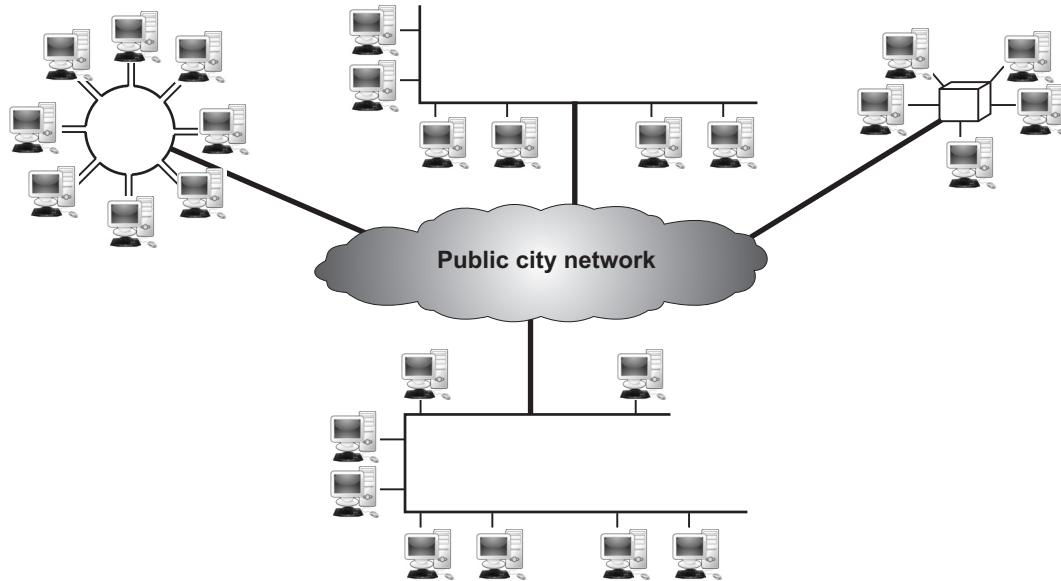
1. The reliability of LAN is high because the failure of one computer in the network does not affect the functioning for other computers.
2. Addition of a new computer to the network is easy and simple.
3. High rate of data transmission is possible.
4. Peripheral devices like magnetic disk, printer etc. 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 unauthorized users from using programs and data.
4. LANs need to be maintained by skilled technicians.
5. In LAN if the file server develops a serious fault, all the users are affected.

1.2.5.2 Metropolitan Area Networks (MAN)

- When the need for connecting a larger number of computers into a single network arises, the network spreads to a larger area comprising a metropolitan area then it is known as Metropolitan Area Network (MAN).
- A MAN is a computer network that interconnects users with computer resources in a geographic region of the size of a metropolitan area like the entire city.
- If a network spans 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.
- A MAN connects networks within a city or metropolitan size area. Geographical area for MAN lies between 5 km to 50 km generally covers towns and cities.
- A MAN is designed for customers who need a high-speed connectivity, normally to the Internet, and have endpoints spread over a city or part of the city.
- In MAN networks data is transmitted over one or two cables. A good example of a MAN is the part of the telephone company network that can provide a high-speed DSL line to the customer.
- The MAN was designed and developed to cover an entire city and the range of MAN is greater compared to LAN setup. MAN can connect several LANs to form a larger network (See Fig. 1.21).

**Fig. 1.21: 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 used in MAN.

Advantages:

1. MAN spans a large geographical area (5 to 50 km) 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. Implementation cost is high.
2. Speed is slow.
3. In MAN there are high chances of attacking hackers on the network compared to LAN. So data may be leaked.
4. To set up MAN it requires technical people that can correctly set up MAN.

1.2.5.3 Wide Area Networks (WAN)

- The need for the growth of computer networks to global proportions leads to the Wide Area Network (WAN).
- A large number of autonomous computers are located over a large remote geographical area called WAN.
- The main feature of WAN is that computers are located in different geographical areas and each is connected to the main network.
- 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.
- A WAN is a geographically-dispersed collection of LANs. A wide area network is simply a LAN of LANs or Network of Networks.
- WANs are characterized by the slowest data communication rates and the largest distances.
- WANs are commonly connected either through the Internet or special arrangements made with phone companies or other service providers.
- The Internet is the largest WAN, spanning the World today. Fig. 1.22 shows a typical WAN.

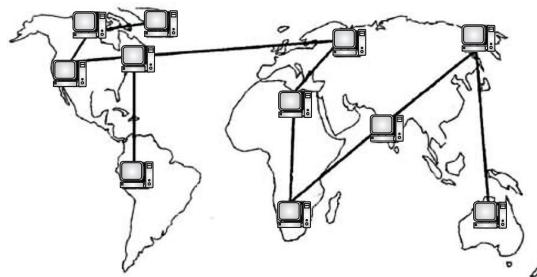


Fig. 1.22: WAN

- 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. 1.23 shows communication Subnet and Host is WAN.

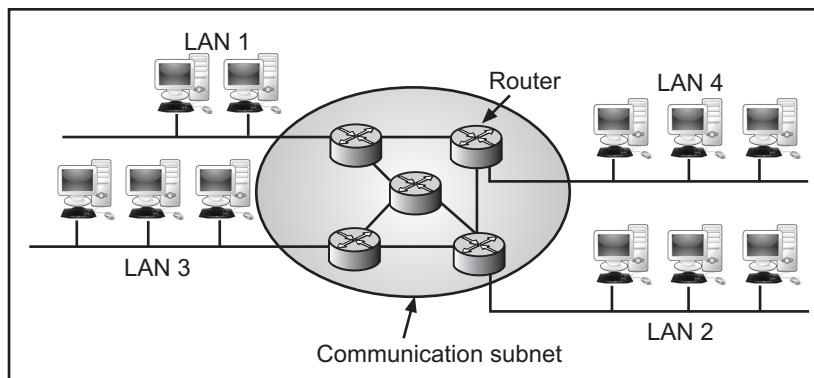


Fig. 1.23: Communication Subnet and Host is WAN

- The function of the subnet is to carry messages from host to host. The subnet consists of two important components; namely, 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 arrives 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 an 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 an enterprise network.
- The transmission in WAN is based on a point-to-point technology involving the process of switching.

Point-to-Point WAN:

- A point-to-point WAN is a network that connects more than two communicating devices through a transmission media like cable or air.
- The point-to-point WAN is normally a line leased from a telephone or cable TV provider that connects a home computer or a small LAN to an Internet Service Provider (ISP).
- A point-to-point WAN is often used to provide Internet access. Fig. 1.24 shows an example of a point-to-point WAN.

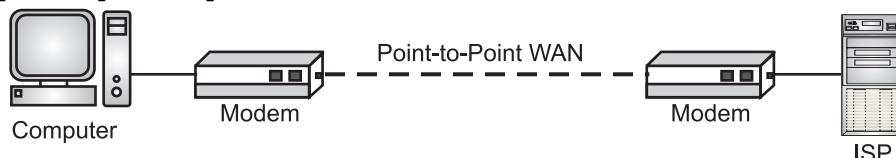


Fig. 1.24: Point-to-Point WAN

Switched WAN:

- The switched WAN connects the end systems and is used in the backbone of global communication today.
- Switched WAN is a combination of several point-to-point WANs that are connected by switches.
- Fig. 1.25 shows an example of a switched WAN. Examples of switched WAN includes asynchronous transfer mode (ATM) network, Wireless WAN.

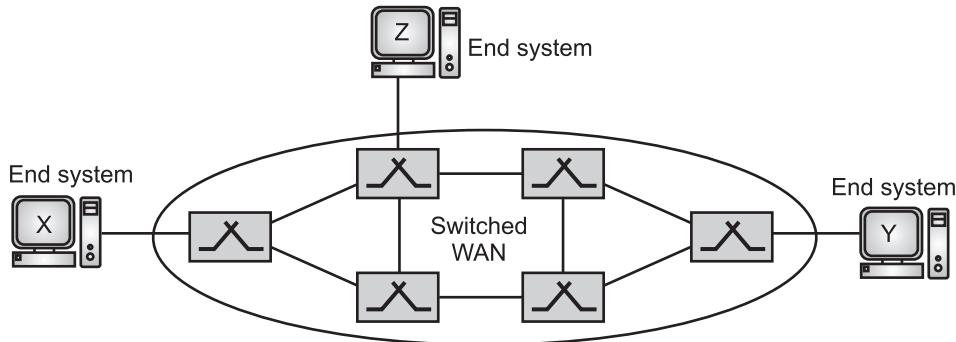


Fig. 1.25: Switched WAN

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 user's information communication.

Disadvantages of WAN:

1. WANs are expensive.
2. WANs need a good firewall to restrict outsiders from entering and disrupting the network.
3. Setting up a network can be an expensive and complicated experience. The bigger the network the more expensive it is.
4. Security is a real issue when many different people have the ability to use information from other computers. Protection against hackers and viruses adds more complexity and expense.
5. Slower than LAN and MAN.

Difference between LAN, MAN and WAN:

(April 17)

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 areas, like country, state etc.	Covers larger areas than LAN and smaller than WAN like cities.

Contd...

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. Set-up cost	Low.	High.	Moderate.
9. Ownership	Owned by private organizations.	Ownership can be private or public.	Ownership can be private or public.
10. Designing and Maintenance	Easy and less costly than WAN.	Complex and more costly than LAN.	Complex and more costly than LAN.

1.2.5.4 Internetwork

(April 16)

- When two or more separate networks are connected for exchanging data or resources, they become an internetwork (or internet).
- 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 computer internetworking.
- 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.
- An internetwork is a collection of individual networks, connected by intermediate networking devices, that functions as a single large network.
- For example, assume that an organization has two offices, one on the east coast and the other on the west coast.
- Each office has a LAN that allows all employees in the office to communicate with each other.
- To make the communication between employees at different offices possible, the office management leases a point-to-point dedicated WAN from a service provider, such as a telephone company, and connects the two LANs.

- Now the company has an internetwork, or a private internet (with lowercase i) and the communication between offices is now possible. Fig. 1.11 shows this internetwork or internet.

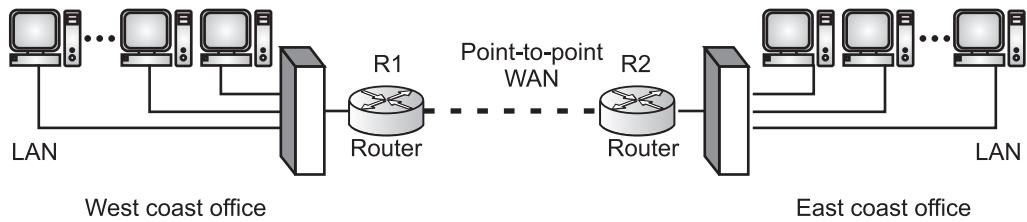


Fig. 1.26: An internetwork made up of Two LANs and One Point-to-Point WAN

- When a host in the west coast office sends a message to another host in the same office, the router blocks the message, but the switch directs the message to the destination.
- On the other hand, when a host on the west coast sends a message to a host on the east coast, router R1 routes the packet to router R2, and the packet reaches the destination.
- Fig. 1.27 shows another internet with several LANs and WANs connected. One of the WANs is a switched WAN with four switches.

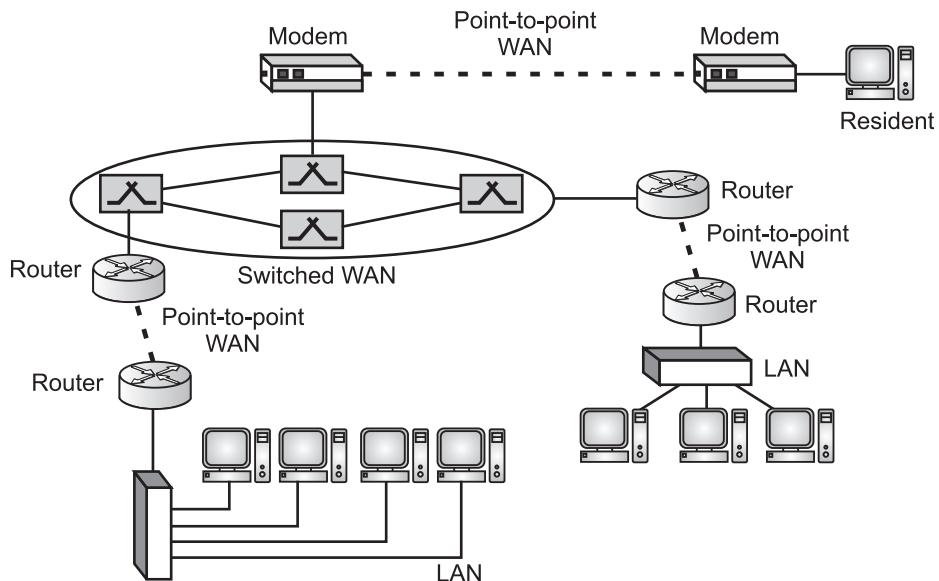


Fig. 1.27: A Heterogeneous Network made of Four WANs and Three LANs

- 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 two 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. Intranet is a private network that is set up within an organization and also controlled by the organization, nobody outside of the organization is permitted to access the network.
 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. Extranet is an extended intranet owned, operated and controlled by an organization. In addition to allow access to members of an organization, an extranet uses firewalls, access profiles and privacy protocols to allow access to users from outside the organization.

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 distances by connecting multiple smaller networks.

1.2.6 Switching

- An internet is a switched network in which a switch connects at least two links together. A switch needs to forward data from a network to another network when required.
- The two most common types of switched networks are circuit-switched network and packet-switched network.

1.2.6.1 Circuit-Switched Network

- In a circuit-switched network, a dedicated connection, (called a circuit) is always available between the two end systems; the switch can only make it active or inactive.
- Fig. 1.28 shows a very simple switched network that connects four telephones to each end.
- We have used telephone sets instead of computers as an end system because circuit switching was very common in telephone networks in the past, although part of the telephone network today is a packet-switched network.

- In Fig. 1.28, the four telephones at each side are connected to a switch. The switch connects a telephone set at one side to a telephone set at the other side.
- The thick line in Fig. 1.28 connecting two switches is a high-capacity communication line that can handle four voice communications at the same time; the capacity can be shared between all pairs of telephone sets.
- The switches used in this example have forwarding tasks but no storing capability.

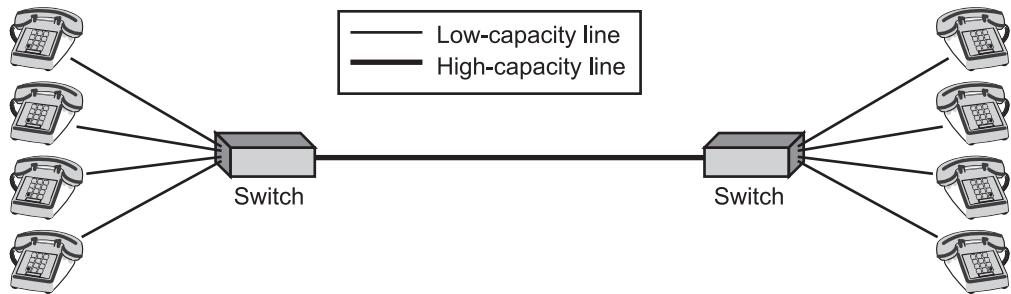


Fig. 1.28: A Circuit Switched Network

- Let us look at following two cases in a circuit-switched network:
 - Case 1:** In this case, all telephone sets are busy; four people at one site are talking with four people at the other site; the capacity of the thick line is fully used.
 - Case 2:** In this case, only one telephone set at one side is connected to a telephone set at the other side; only one-fourth of the capacity of the thick line is used.
- This means that a circuit-switched network is efficient only when it is working at its full capacity; most of the time, it is inefficient because it is working at partial capacity.
- The reason that we need to make the capacity of the thick line four times the capacity of each voice line is that we do not want communication to fail when all telephone sets at one side want to be connected with all telephone sets at the other side.

1.2.6.2 Packet-Switched Network

- In a computer network, the communication between the two ends is done in blocks of data known as packets.
- In other words, instead of the continuous communication we see between two telephone sets when they are being used, we see the exchange of individual data packets between the two computers.
- This allows us to make the switches function for both storing and forwarding because a packet is an independent entity that can be stored and sent later.
- Fig. 1.29 show a small packet-switched network that connects four computers at one site to four computers at the other site.
- A router in a packet-switched network has a queue that can store and forward the packet.

- Now assume that the capacity of the thick line is only twice the capacity of the data line connecting the computers to the routers.
- If only two computers (one at each site) need to communicate with each other, there is no waiting for the packets.
- However, if packets arrive at one router when the thick line is already working at its full capacity, the packets should be stored and forwarded in the order they arrived.
- The two simple examples show that a packet-switched network is more efficient than a circuit-switched network, but the packets may encounter some delays.

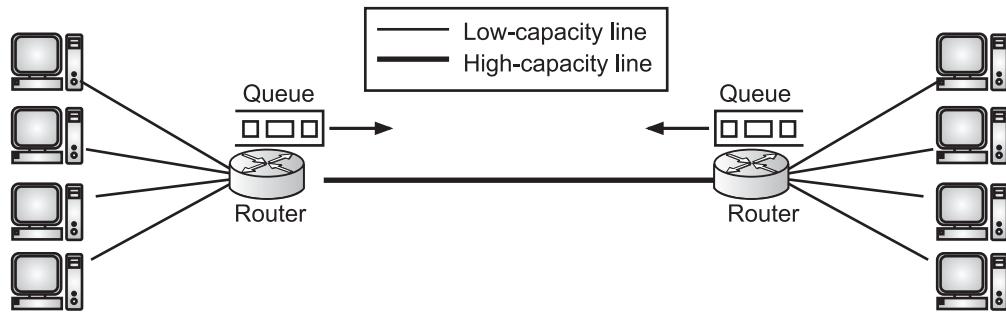


Fig. 1.29: A Packet-Switched Network

1.2.7 Internet

- The term Internet is derived from the words ‘interconnection’ and ‘networks’. The Internet is also known as ‘Net’.
- A network is a collection of two or more computers, which are connected together to share information and resources.
- The Internet is a worldwide system of computer networks, i.e. network of networks.
- Through the Internet, computers become able to exchange information with each other and find diverse perspectives on issues from a global audience.
- The Internet is the global system of interconnected computer networks that uses the Internet protocol suite (TCP/IP) to communicate between networks and devices.
- The Internet is a network of networks that consists of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies.
- An internet (note the lowercase i) is two or more networks that can communicate with each other. The most notable internet is called the Internet (uppercase I) and is composed of thousands of interconnected networks.
- Fig. 1.30 shows a conceptual (not geographical) view of the Internet which shows the Internet as several backbones, provider networks, and customer networks.
- At the top level, the backbones are large networks owned by some communication companies like Sprint, Verizon (MCI), AT&T, and so on.

- The backbone networks are connected through some complex switching systems, called peering points. At the second level, there are smaller networks, called provider networks, that use the services of the backbones for a fee.
- The provider networks are connected to backbones and sometimes to other provider networks. The customer networks are networks at the edge of the Internet that actually use the services provided by the Internet.
- The customer networks pay fees to provider networks for receiving services. Backbones and provider networks are also called Internet Service Providers (ISPs).
- The backbones are often referred to as international ISPs, the provider networks are often referred to as national or regional ISPs.

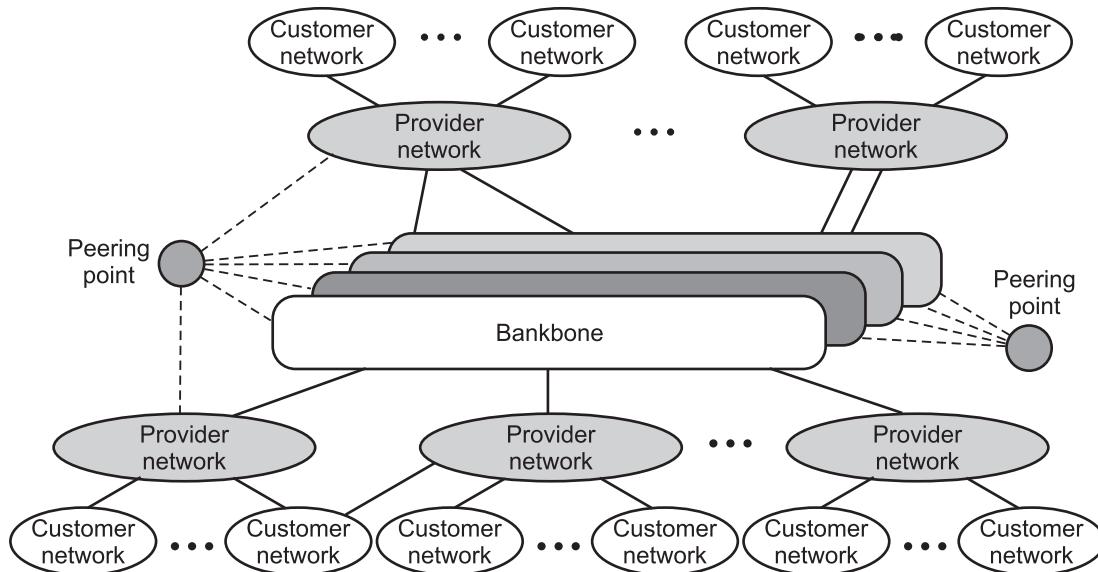


Fig. 1.30: The Internet Today

1.2.7.1 Accessing the Internet

- Internet access is the ability of individuals and organizations to connect to the Internet using computer terminals, computers, and other devices; and to access services such as email and the World Wide Web (WWW).
- Internet access is sold by Internet Service Providers (ISPs) delivering connectivity at a wide range of data transfer rates via various networking technologies.
- The Internet today is an internetwork that allows any user to become part of it. The user, however, needs to be physically connected to an ISP. The physical connection is normally done through a point-to-point WAN.
- In this section we will study various ways to access the Internet.

1. Using Telephone Networks:

- Today a number of residences and small businesses/organizations have telephone service, which means they are connected to a telephone network.
- Since, most telephone networks have already connected themselves to the Internet, one option for residences and small businesses/organizations to connect to the Internet is to change the voice line between the residence or business and the telephone center to a point-to-point WAN.
- This can be done in following two ways:

(i) Dial-up Service: Dial-up connection uses telephone lines to connect PCs to the internet. It requires a modem to set up dial-up connection. This modem works as an interface between PC and the telephone line. The modem connects the computer through the standard phone lines, which serves as the data transfer medium. The modem converts data to voice. The software installed on the computer dials the ISP and imitates making a telephone connection. Unfortunately, the dial-up service is very slow, and when the line is used for Internet connection, it cannot be used for telephone (voice) connection. It is only useful for small residences. Fig. 1.31 shows typical dial-up connection.

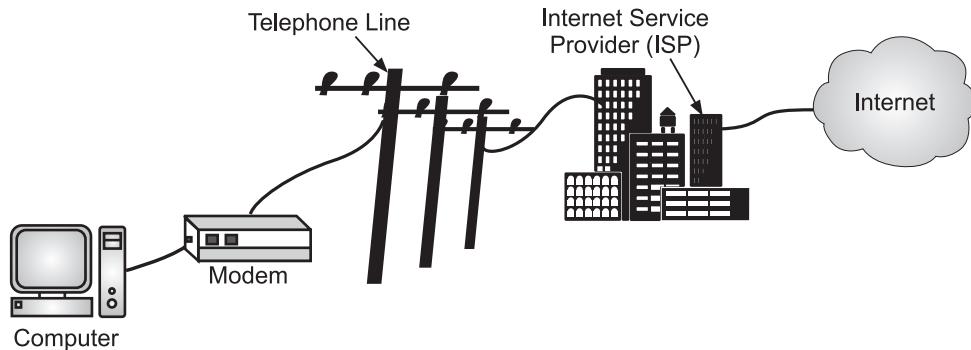


Fig. 1.31: Dial-up Connection/Access of Internet

(ii) DSL Service: Digital Subscriber Line (DSL) service provides a connection to the Internet through the telephone network. Unlike dial-up, DSL can operate using a single phone line without preventing normal use of the telephone line for voice phone calls. DSL uses the high frequencies, while the low (audible) frequencies of the line are left free for regular telephone communication. Since the advent of the Internet, some telephone companies have upgraded their telephone lines to provide higher speed Internet services to residences or small businesses/organizations. The DSL service also allows the line to be used simultaneously for voice and data communication. Faster forms of DSL, are also available like High Data Rate Digital Subscriber Line (HDSL), Very High Data Rate

Digital Subscriber Line (VHDSL), Asymmetric Digital Subscriber Line (ADSL), Symmetric DSL (SDSL) and so on. Fig. 1.32 shows a sample connection diagram for typical residential DSL.

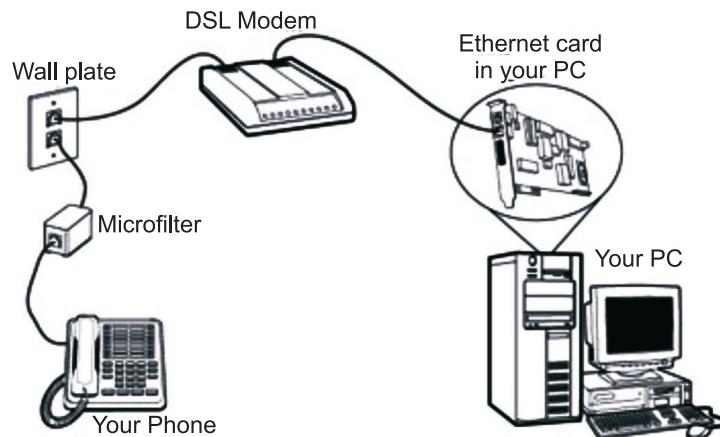


Fig. 1.32: Typical Residential DSL Connection/Access of Internet

Here, are some key points to note in Fig. 1.32:

- Connect your DSL modem's data connection to the phone jack on a wall plate.
- Connect the DSL modem's Ethernet connection to the Ethernet card on your PC.
- When you connect other telephones or fax machines on the same phone line, install a micro-filter between the wall plate and each of these devices.

2. Using Cable Networks:

- Now-a-days many cable television companies use some percentage of their network's bandwidth to provide internet access through prevailing cable television connections.
- Since this connection uses a special cable modem, it is called "Cable Modem Service". A cable modem can be added to or integrated with a set-top box that provides the TV set for Internet access.
- Cable television systems transmit data via coaxial cable, which can transmit data as much as 100 times faster than common telephone lines.
- More and more residents over the last two decades have begun using cable TV services instead of antennas to receive TV broadcasting.
- The cable companies have been upgrading their cable networks and connecting to the Internet. A residence or a small business can be connected to the Internet by using this service.
- It provides a higher speed connection, but the speed varies depending on the number of neighbors that use the same cable.

- Fig. 1.33 shows how internet is accessed using Cable TV connection. A cable modem is used to access this service, provided by the cable operator.
- The Cable modem comprises two connections: one for internet service and other for Cable TV signals.
- Since Cable TV internet connections share a set amount of bandwidth with a group of customers, therefore, data transfer rate also depends on the number of customers using the internet at the same time.

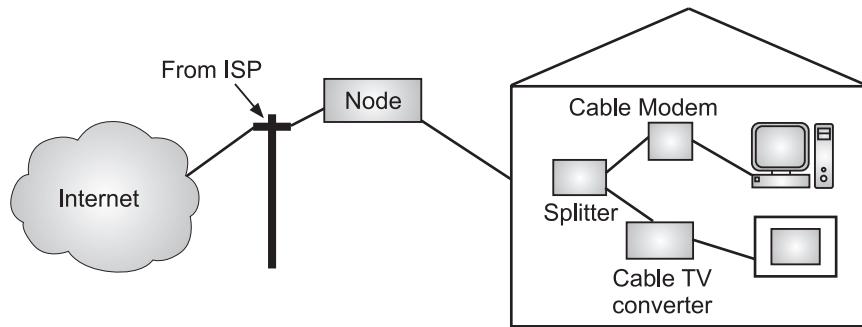
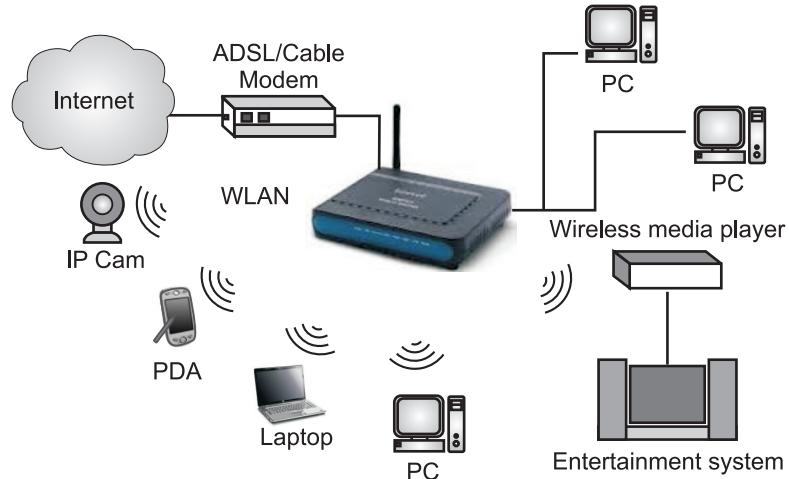


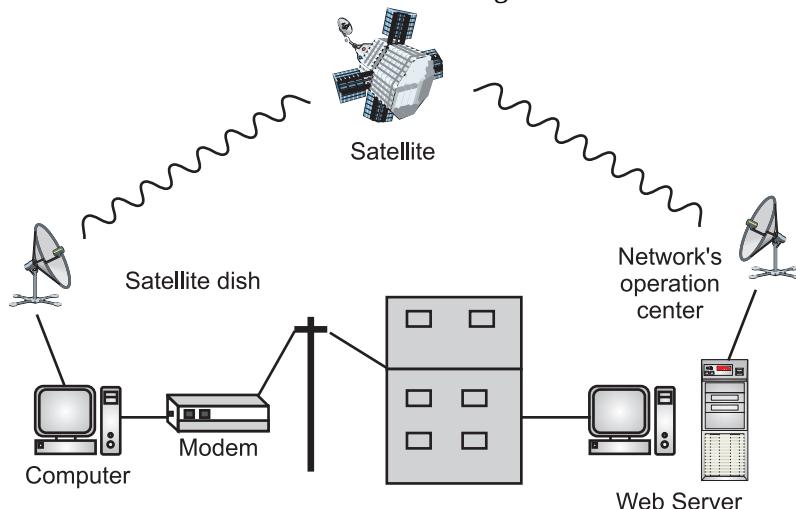
Fig. 1.33: Typical Residential Cable TV Connection/Access of Internet

3. Using Wireless Networks:

- Now-a-days Wireless connectivity has recently become increasingly popular. A household or a small business/organization can use a combination of wireless and wired connections to access the Internet.
- Wireless Internet connection makes use of radio frequency bands to connect to the Internet and offers a very high speed. The wireless internet connection can be obtained by either Wi-Fi or Bluetooth.
- Wireless LAN (WLAN) connections are very common these days, which are based on the technology that is often cited as Wi-Fi (Wireless Fidelity). WLANs are based on IEEE 802.11 standards.
- To connect to the internet, the wireless access point is connected to a wired LAN like any other devices, and then computers with wireless NICs can access the wired LAN.
- With the growing wireless WAN access, a household or a small business can be connected to the Internet through a Wireless WAN (WWAN).
- A WWAN accepts and transmits data using radio signals via cellular sites and satellites.
- Satellite Internet connection offers high speed connection to the internet. There are two types of satellite internet connection namely one-way connection or two-way connection.
- In a one-way connection, we can only download data but if we want to upload, we need dialup access through an ISP over telephone line.

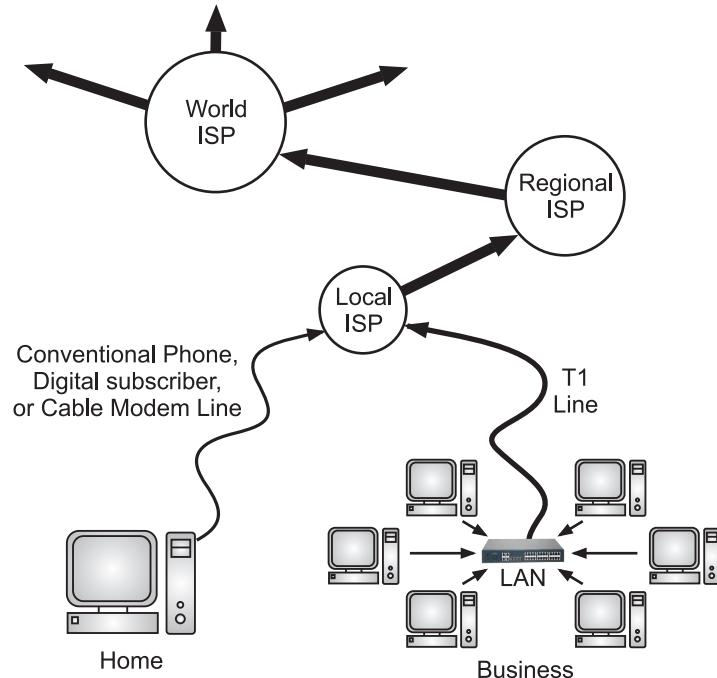
**Fig. 1.34: WLAN Internet Connection/Access of Internet**

- In two-way connection, we can download and upload the data by the satellite. It does not require any dialup connection.
- Fig. 1.35 shows how the internet is accessed using satellite internet connection.

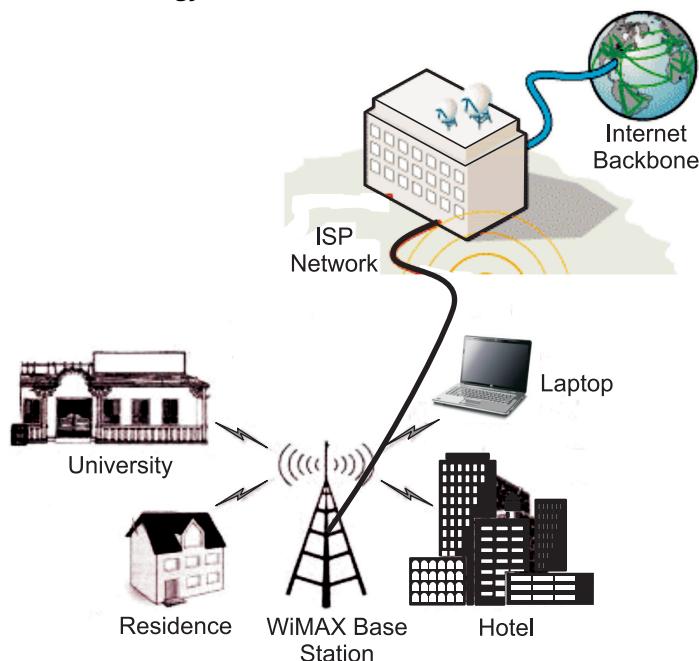
**Fig. 1.35: WWAN Satellite Internet Connection/Access of Internet**

4. Direct Connection to the Internet:

- A large organization or a large corporation can itself become a local ISP and be connected to the Internet.
- This can be done if the organization or the corporation leases a high-speed WAN from a carrier provider and connects itself to a regional ISP.
- For example, a large university with several campuses can create an internetwork and then connect the internetwork to the Internet.

**Fig. 1.36: Direct Internet Connection/Access of Internet**

- Today, Worldwide Interoperability for Microwave Access (WiMAX) is one of the popular wireless technology.

**Fig. 1.37: WiMax Internet Connection/Access of Internet**

- WiMax is a Wireless MAN (WMAN) technology. WiMAX can provide at-home or mobile Internet access across whole cities or countries.
- WiMAX would operate similar to Wi-Fi but at higher speed, over greater distances and for a greater number of users.
- WiMax Internet access is used by businesses/organizations to provide reliable, dedicated service for Internet access as well as other applications including e-mail, file sharing, web hosting, data backup, video and so on.

1.2.8 Advantages, Disadvantages and Applications of Network

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

Advantages of Computer Network:

1. **Easy Communication:** A computer network allows all the network users or computers at a different location to communicate easily. The network users can communicate with each other using e-mails, instant messaging, video conferencing, chat rooms, blogging etc.
2. **Ability to Share Files, Data and Information:** The computer network has the ability to share data/files and information to users or computers connected to the computer network.
3. **Flexible Access:** Access of files from computers throughout the world, and 24×7 environment.
4. **Backup and Recovery:** Generally, in networking the server is placed in a secure place and the good mechanism is providing for backup of data. If the data is lost accidentally or due to any other reason, then it is possible to restore them from the server.
5. **Sharing Hardware:** By using networking we can share the hardware resources in an organization and anywhere. 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 organization. This will significantly reduce the cost of purchasing hardware.
6. **Instant and Multiple Accesses:** Computer networking enables multiple users to access the same data at the same time from a same or remote location. For example, a World Wide Web (WWW) in which everyone can access a web page from a different location and read the same information at a same time.
7. **Sharing Software:** Users can share software within the network easily. Networkable versions of software are available at considerable savings compared

to individually licensed versions of the same software. Therefore, large organizations can reduce the cost of buying software by networking their computers.

8. **Security:** Network security issues consist of prevention from virus attacks and protecting data from unauthorized access. Sensitive files and programs on a network can be password protected. Only authorized users can access resources in a computer network.
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 of Computer Network:

1. **Expensive to Build:** Building a network is complex and time consuming for large scale organizations.
2. **Virus and Malware:** Viruses can spread on a network easily, because of the inter-connectivity of workstations.
3. **Lack of Robustness:** If the main file server of a computer network breaks down, the entire system becomes down and useless.
4. **Needs an Efficient Handler:** The technical skills and knowledge required to operate and administer a computer network.
5. **High Cost:** The investment for hardware and software can be costly for initial set-up of computer networks.
6. **Security Threats:** Security threats are always problems with computer networks. There are hackers who are trying to steal valuable data/information of large organizations for their own benefit.

Applications of Computer Network:

1. **Marketing and Sales:** Computer networks are used extensively in both marketing and sales organizations. Marketing professionals use them to collect, exchange, and analyze data related to customer needs and product development cycles. Sales application includes teleshopping, which uses order-entry computers or telephones connected to order processing networks, and online-reservation services for hotels, airlines and so on.
2. **Financial Services:** Today's financial services are totally dependent on computer networks. Application includes credit history searches, foreign exchange and investment services, and electronic fund transfer, which allow users to transfer money without going into a bank (an Automated Teller Machine (ATM) is an example of electronic fund transfer automatic pay-check is another).

3. **Manufacturing:** Computer networks are used in many aspects of manufacturing including the manufacturing process itself. Two of them that use networks to provide essential services are Computer-Aided Design (CAD) and Computer-Assisted Manufacturing (CAM), both of which allow multiple users to work on a project simultaneously.
4. **Directory Services:** Directory services allow lists of files to be stored in a central location to speed worldwide search operations.
5. **Information Services:** A Network information services includes bulletin boards and data banks. A World Wide Web (WWW) site offering technical specification for a new product is an information service.
6. **Electronic Data Interchange (EDI):** EDI allows business information, including documents such as purchase orders and invoices, to be transferred without using paper.
7. **Electronic Mail:** Probably it's the most widely used computer network application.
8. **Teleconferencing:** Teleconferencing allows conferences to occur without the participants being in the same place. Applications include simple text conferencing (where participants communicate through their normal keyboards and monitor) and video conferencing where participants can even see as well as talk to other fellow participants.
9. **E-Commerce:** Computer networks have paved the way for a variety of business and commercial transactions online, popularly called e-commerce. Users and organizations can pool funds, buy or sell items, pay bills, manage bank accounts, pay taxes, transfer funds and handle investments electronically.

1.3 NETWORK SOFTWARE

- In computer networks, not only the hardware but software is also very important. For communication between devices, hardware and software both are required.
- Traditional networks were hardware based with software embedded. Network software is now highly structured.
- Network software encompasses a broad range of software used for design, implementation, and operation and monitoring of computer networks.
- Networking software, in the most basic sense, is software that facilitates, enhances or interacts with a computer network.
- One type of networking software allows computers to communicate with one another, while another type of networking software provides users access to shared programs.
- Networking software is a key component of today's computer networks, including the Internet.

- Network software is a general phrase for software that is designed to help set up, manage, and/or monitor computer networks.
- Networking software applications are available to manage and monitor networks of all sizes, from the smallest home networks to the largest enterprise networks.

Functions of Network Software:

1. Helps to set up and install computer networks.
 2. Enables users to have access to network resources in a seamless manner.
 3. Allows administrations to add or remove users from the network.
 4. Helps to define locations of data storage and allows users to access that data.
 5. Helps administrators and security systems to protect the network from data breaches, unauthorized access and attacks on a network.
- With the advent of Software Defined Networking (SDN), software is separated from the hardware thus making it more adaptable to the ever-changing nature of the computer network.

1.3.1 Protocol Hierarchies

- In a computer network, many devices are connected to each other. Every computer is working as a source or destination or intermediate machine.
- It is also possible that a computer is simultaneously performing all these jobs. As a source, destination or intermediate machine certain predefined jobs a computer has to perform. The entire structure of a computer network is complex.
- To reduce their design complexity, networks are organized as a stack of layers or levels, each one built upon the one below it.
- The number of layers, the name of each layer, the contents of each layer and the function of each layer differ from network to network. Each layer offers certain predefined services to higher layers and taking services from lower layers.
- The basic concept of layering network responsibilities is that each layer adds value to services provided by sets of lower layers.
- In this way, the highest level is offered the full set of services needed to run a distributed data application.
- Fig. 1.38 shows a layered architecture where layer n at the source logically (but not necessarily physically) communicates with layer n at the destination and layer n of any intermediate nodes.
- Layer n on one machine carries on a conversation with layer n on another machine. The rules and conventions used in this conversation are collectively known as the layer n protocol.

- A protocol is an agreement between the communicating parties on how communication is to proceed.
- A five-layer network is shown in Fig. 1.38. The entities comprising the corresponding layers on different machines are called peers.
- The peers may be processes, hardware devices or even human beings. It is the peers that communicate by using the protocol.
- In reality, no data are directly transferred from layer n on one machine to layer n on another machine.
- Each layer passes data and control information to the layer immediately below it, until the lowest layer is reached. Below layer 1 is the physical medium through which actual communication occurs.
- In Fig. 1.38 virtual communication is shown by dotted lines and physical communication by solid lines.
- Between each pair of adjacent layers is an interface. The interface defines which primitive operations and services the lower layer gives to the upper layer.
- A set of layers and protocols is called a network architecture.
- The details of implementation and the specification of the interfaces is not part of architecture because they are hidden inside the machines and not visible from outside.
- A list of protocols used by a certain system, one protocol per layer, is called a protocol stack.

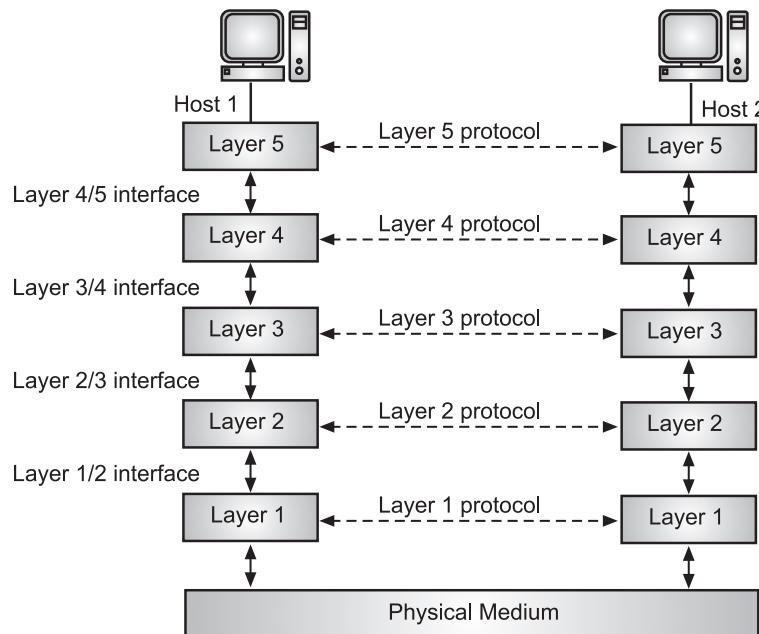


Fig. 1.38: Layers, Protocols and Interfaces

- To understand the idea of multilayer communication, consider the example of post office.

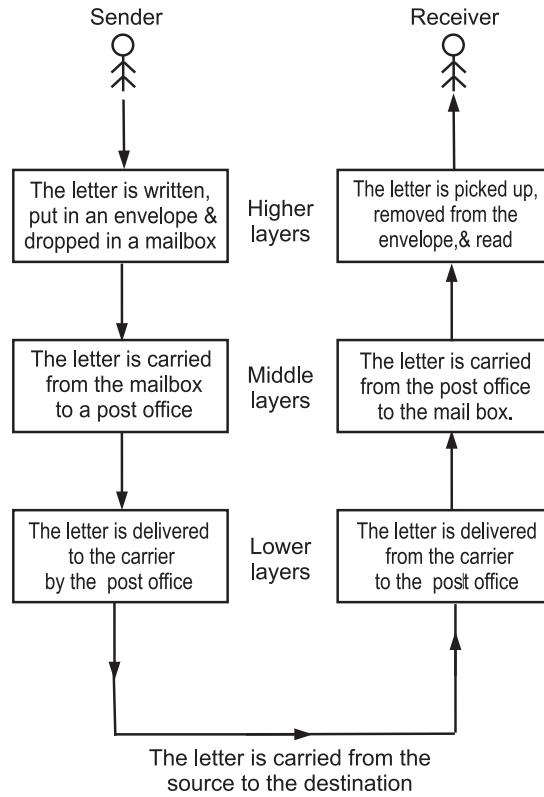


Fig. 1.39

- Now, we will discuss a more technical example of how to provide communication to the top layer of the five-layer network.
- A message M, is produced by an application process running in layer 5 and given to layer 4 for transmission. Layer 4 adds a header part i.e. control information in front of the message and passes the message to layer 3.
- The control information may include sequence number, source address, destination address, total number of bytes etc.
- We assume that layer 3 is not able to handle large data, so layer 3 breaks-up the incoming messages into smaller units (Packets), adding layer 3 header to it and gives to layer 2. In our example, M is split into two parts M1 and M2.
- Layer 2 adds not only a header, but also a trailer (which is also a control information) to it and passes to layer no. 1 for physical transmission.
- At the receiving machine, the message is received by layer 1 and then moves upward from layer to layer.

- Every layer removes the header part attached by the corresponding layer from the sender's machine. None of the headers for layers below n are passed up to layer n.

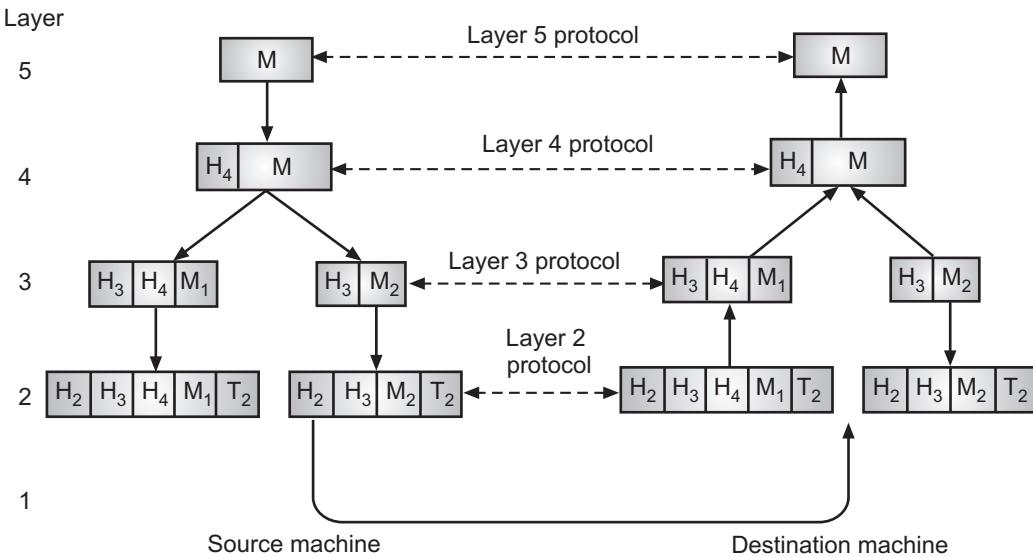


Fig. 1.40: Data Flow between Machines

1.3.2 Design Issues of the Layers

- A network consists of a series of levels called layers. The various key design issues are present in several layers in computer networks.
- Some of the main design issues in layers are as follows:
 - Addressing:** Every layer needs a mechanism for identifying senders and receivers. In computer networks from many computers, some of which have multiple processes, some sort of mechanism is needed for a process on one machine to specify with whom it wants to talk. As a consequence of having multiple destinations, some form of addressing is needed in order to specify a specific destination.
 - Data Transfer Methods:** Data transfer means sending data from one computer to another. In computer networks, data transfer can be of three modes i.e. simplex, half duplex and full duplex.
 - Error Control:** Error control is an important issue because physical communication channels are not perfect. Many error-detecting and error-correcting codes are known, but both ends of the connection must agree on which one is being used. The receiver must have some way of telling the sender which messages have been correctly received and which have not.
 - Flow Control:** If the sender is fast compared to the receiver, the issue occurs at every layer is how to keep a fast sender from swamping a slow receiver with data.

One solution is both entities agree upon the data rate to control the flow. Another solution involves some kind of feedback from the receiver to the sender about the receiver's current situation. This subject is called flow control.

5. **Disassembling and Reassembling of Messages:** Another problem that must be solved at several levels is the inability of all processes to accept arbitrarily long messages. One solution is to divide long messages into multiple small messages, transmit them and combine them at the receiving end.
6. **Multiplexing and Demultiplexing:** When it is inconvenient or expensive to set up a separate connection for each pair of communicating processes, the underlying layer may decide to use the same connection for multiple, unrelated conversations. This is known as multiplexing. Multiplexing is needed in the physical layer.
7. **Routing:** When multiple paths between source and destination are available, a route must be chosen depending upon certain criteria. Criteria may be current traffic or situation of the subnet. Criteria is called a routing protocol and this process is called routing.
8. **Order of Messages:** Not all communication channels preserve the order of messages sent on them. To deal with possible loss of sequencing, the protocol must make explicit provision for the receiver to allow the pieces to be reassembled properly.
9. **Scalability:** Networks are continuously evolving. The sizes are continually increasing leading to congestion. Also, when new technologies are applied to the added components, it may lead to incompatibility issues. Hence, the design should be done so that the networks are scalable and can accommodate such additions and alterations.
10. **Security:** A major factor of data communication is to defend it against threats like eavesdropping and surreptitious alteration of messages. So, there should be adequate mechanisms to prevent unauthorized access to data through authentication and cryptography.
11. **Resource Allocation:** Computer networks provide services in the form of network resources to the end users. The main design issue is to allocate and deallocate resources to processes. The allocation/deallocation should occur so that minimal interference among the hosts occurs and there is optimal usage of the resources.

1.3.3 Connection-Oriented and Connection-less Services

- Layers can offer two types of services to the layers above them namely connection-oriented service and connection-less service.

1.3.3.1 Connection-Oriented Services

- In connection-oriented service, logical connection is established between communicating parties. Connection oriented service is modeled after the telephone system.
- In the telephone system, when we want to make a call, we have to pick up the phone, dial the number, after that connection is established, use that connection and then disconnect the telephone.
- To use a connection oriented network service, the service user first establishes a connection, uses the connection and then releases the connection. Once, the connection is established between source and destination, the path is fixed.
- The data transmission takes place through this path established. The order of the messages sent will be the same at the receiver end.
- Services are reliable and there is no loss of data. Most of the time, reliable service provides acknowledgement as an overhead and adds delay.

Basic Working Concept of Connection-Oriented Service:

- The connection-oriented service first establishes the virtual connection between the source and the destination.
- Then transfers all data packets belonging to the same message through the same dedicated established connection and after all packets of a message are transferred it releases the connection.

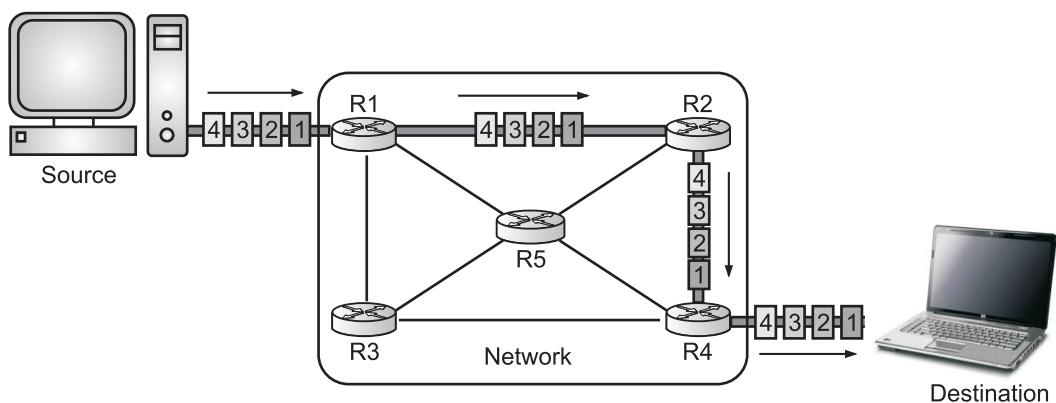


Fig. 1.41: Connection-oriented Service

- To establish a connection a source sends a request packet to the destination. In response to which destination sends the acknowledgement packet to the source confirming that the destination is ready to accept the data from the source.

- The routers involved in the exchange of request and acknowledgement packets between source and destination, define the virtual path that will be followed by all packets belonging to the same message.

Advantages of Connection-oriented Services:

1. These services provide guaranteed delivery of data.
2. This service is more reliable than connectionless services.
3. Some connection oriented services will monitor for lost packets and handle resending them.

Disadvantages of Connection-oriented Services:

1. A connection must require.
2. These services have more overhead than connectionless service.
3. Complex method for data transferring.

1.3.3.2 Connection-less Services

- Connection-less service is modeled after the postal system. In this type of services, no connection is established between source and destination.
- Here, there is no fixed path. Therefore, the messages must carry a full destination address and each one of these messages are sent independent of each other.
- Messages sent will not be delivered at the destination in the same order. Thus, grouping and ordering is required at the receiver end, and the services are not reliable.
- There is no acknowledgement confirmation from the receiver. Unreliable connectionless service is often called datagram service, which does not return an acknowledgement to the sender.
- In some cases, establishing a connection to send one short message is needed. But reliability is required, and then acknowledgement datagram service can be used for these applications.

Basic Working Concept of Connection-less Service:

- Connection-less service is a method of data transmission between two computers in a different network. Connectionless service is also termed as datagram service.
- The connection-less service look-alike the postal system where each letter carries its source and destination address and each one of them is routed through a different path.
- The source divides the message into small acceptable packets known as a datagram. These datagrams are individually pushed into the network; each datagram may travel a different path.

- The network considers each datagram or data packet as an independent entity i.e., no relationship is considered between the packets belonging to the same message.
- Each datagram carries its source and destination address. The router uses the destination address to route the datagram to its destination.
- The packets received at the destination may be received out of order. Hence, the datagrams are assembled to recreate the original message.

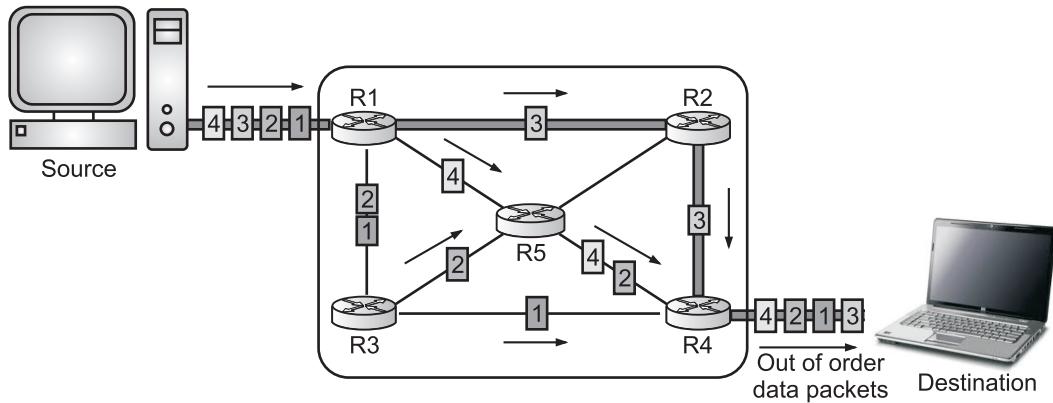


Fig. 1.42: Connection-less Service

Advantages of Connectionless Services:

- Does not require any connection.
- These services are very simple and easy for data transfer.
- Used for periodic burst data transfer.
- Less overhead than connection oriented services.

Disadvantages of Connectionless Services:

- Less reliable than connection-oriented services.
 - No guarantee for delivery of data.
 - It provides minimal services.
- Following table describes various services and examples of connection oriented and connectionless services.

	Service	Example
Connection-Oriented	Reliable message stream	Sequence of pages
	Reliable byte stream	Remote login
Connection-Less	Unreliable connection	Digitized voice
	Unreliable datagram	Electronic junk mail
	Acknowledged datagram	Registered mail
	Request-reply	Database query

Difference between Connectionless and Connection-oriented Services:

Sr. No.	Characteristic	Connectionless Service	Connection-oriented Service
1.	Connection setup	Data is sent without setup i.e. connectionless.	Connection must be established.
2.	Example of protocol	UDP (User Datagram Protocol)	TCP (Transmission Control Protocol).
3.	General description	Simple, high-speed, low functionality "wrapper" that interfaces applications to the network layer.	Full-featured protocol that allows applications to send data reliably without worrying about network layer issues.
4.	Data interface to application	Message-based; data is sent in discrete packages by the applications.	Stream-based; data is sent by the application with no particular structure.
5.	Reliability and acknowledgments	Unreliable, best efforts delivery without acknowledgments	Reliable delivery of messages; all data is acknowledged.
6.	Retransmission	Not performed. Application must detect lost data and retransmit if needed.	Delivery of all data is managed and lost data is retransmitted automatically.
7.	Features provide to manage flow of data.	None.	Flow control using sliding windows; window size adjustment heuristics congestion avoidance algorithm.
8.	Data delivery guarantee	Connectionless services do not.	Connection-oriented services provide some level of delivery guarantee.
9.	Overhead	Connectionless networks have less overhead.	Connection-oriented network services have more overhead.
10.	Transmission speed	Very high.	Low.

Contd....

11.	Data quantity suitability	Small to moderate amounts of data.	Small to very large amounts of data.
12.	Packet Route	Packets can follow any route.	Packets follow the same route.

1.4 REFERENCE MODELS

- A reference model in networking is a conceptual layout that describes how communication between devices should occur.
- In order to provide communication among heterogeneous devices, we need a standardized model i.e. a reference model, which would provide us how these devices can communicate regardless of their architecture.
- The purpose of the reference/network model was to define an architectural framework that defines the logical communication tasks that are required to move information between different computer systems.
- For efficient communication, the reference model identifies the tasks involved in inter-computer communication and divides them in logical groups called layers, with each layer performing a specific function.
- A communication system designed in such a manner is referred to as layered architecture. We used the concept of layers in our daily life, for example, consider communication between two friends through postal mail.

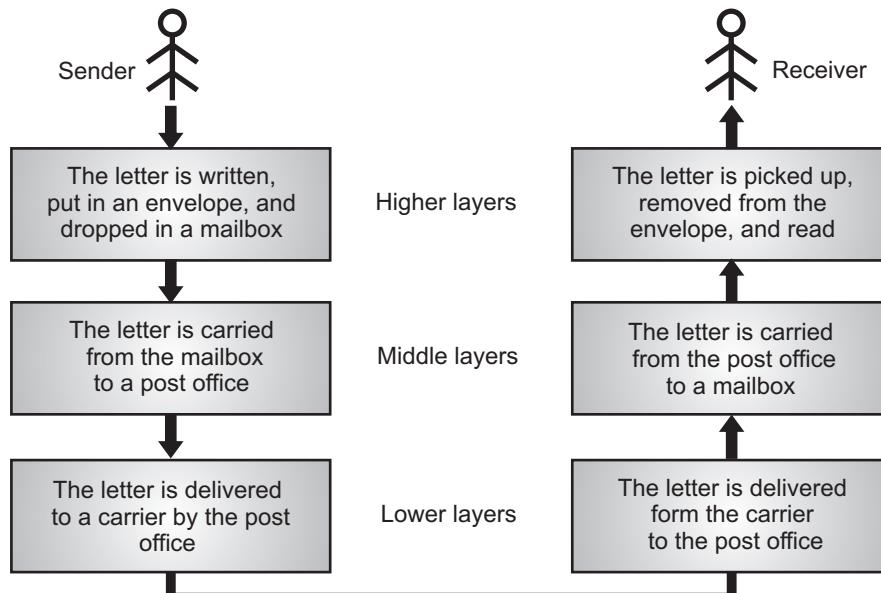


Fig. 1.43: Communication Process

- The process of sending a letter by one friend to another is difficult, if there are no services available by post office.
- In the Fig. 1.43, 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 and site uses services of the layer immediately below it.
- There are two computer network models namely, OSI Model and TCP/IP Model on which the whole data communication process relies. In this section, we will study these two network models with layers and functions of each layer.

1.4.1 OSI Reference Model

(Oct. 17)

- In 1978, the International Organization for Standardization (ISO) developed an architecture that would allow the devices of different manufacturers to work together to communicate with different operating systems.
- In 1984, the ISO architecture became an international standard known as the Open Systems Interconnection (OSI) reference/network model.
- The model is called the ISO-OSI 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 consists of seven separate but related layers, each of which defines a part of the process of moving information across a network.
- The seven layers of OSI model are physical layer, data link layer, network layer, transport layer, session layer, presentation layer and application layer.
- Fig. 1.44 shows OSI reference/network model. 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.

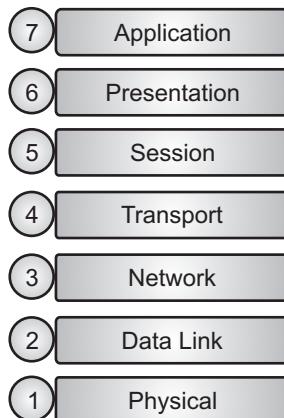


Fig. 1.44: OSI Reference Model

- 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.
- Layers of the OSI model are divided into two groups namely, upper layer and lower layer.
- The upper OSI layers are almost always implemented by software while lower layers are a combination of hardware and software, except the physical layer, which is mostly hardware.
- The upper layers of the OSI model deal with application issues and generally are implemented only in software.
- Generally speaking, software in these layers performs application-specific functions like data formatting, encryption, and connection management.
- The lower layers of the OSI model provide more primitive network-specific functions like routing, addressing, and flow control.
- Upper layers in OSI model are:
 7. Application layer,
 6. Presentation layer, and
 5. Session layer.

- Lower layers in OSI model are:
 4. Transport layer,
 3. Network layer,
 2. Data link layer and
 1. Physical layer.
- The main **benefits of the OSI model** include the following:
 1. Helps users understand the big picture of networking.
 2. Makes troubleshooting easier by separating networks into manageable pieces.
 3. Defines terms that networking professionals can use to compare basic functional relationships on different networks.
 4. Helps users understand how hardware and software elements function together.
 5. Helps users understand new technologies as they are developed.

1.4.1.1 Basic Concepts of OSI Model

- In this section we will study basic concepts in the OSI reference model.

1. 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.

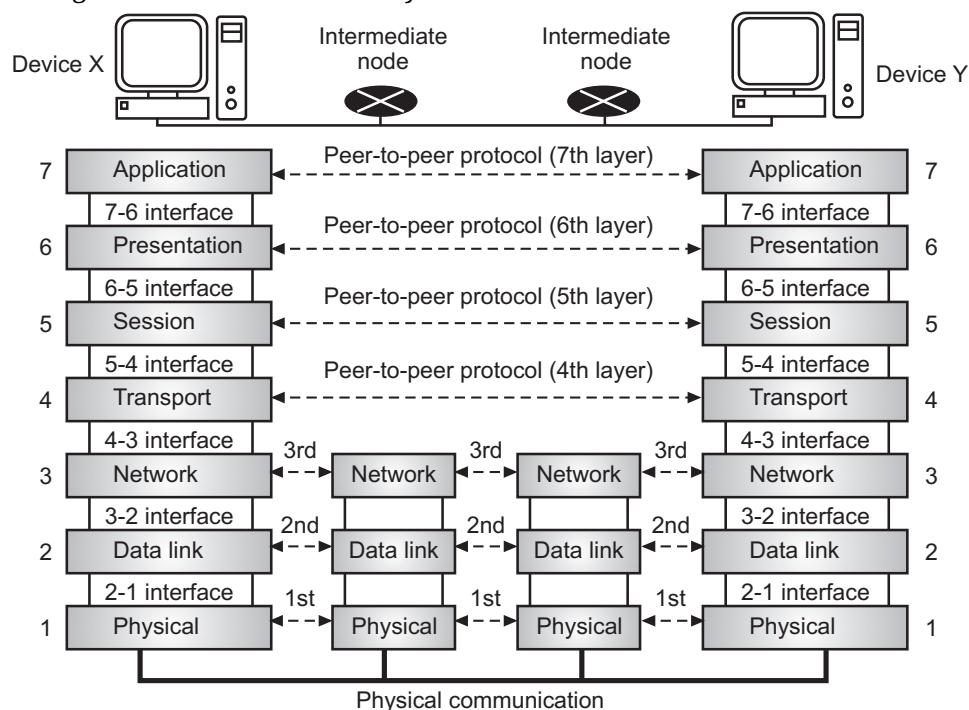


Fig. 1.45: Interactions between OSI model layer or Layered Architecture of OSI Model

- 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.

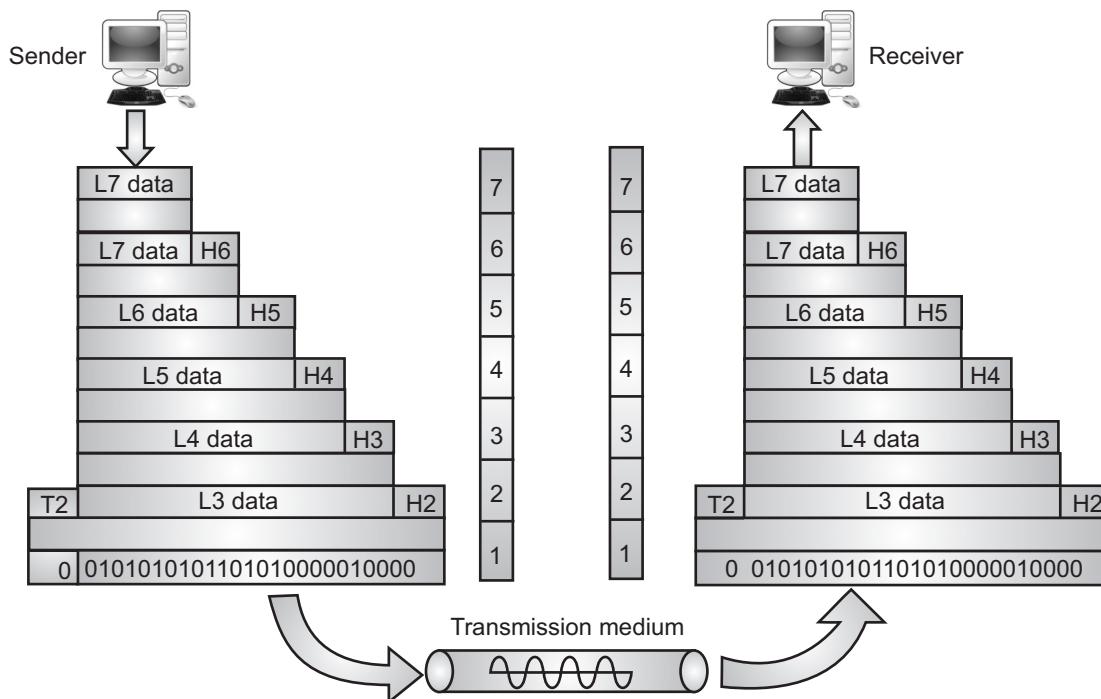


Fig. 1.46: An exchange using OSI model

2. 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.

3. Organization of the Layers:

- All the seven layers are grouped into three subgroups. Layer 1, 2 and 3 are called network support layers 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 allow 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.

1.4.1.2 Functions of Each Layer of OSI Model

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

1. Physical Layer:**(April 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.
- The physical layer also concerned with the following functions:
 - 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.
 - Representation of Bits (Data Encoding):** Below the physical layer there is a transmission medium, which carries computer data. Any transmission medium does not 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 types of encoding methods are used by the Physical layer.
 - Data Rate Control:** Physical layer defines the transmission rate i.e. the number of bits sent in one second. Therefore, it defines the duration of a bit.
 - Bit synchronization:** The physical layer provides the synchronization of the bits by providing a clock. This clock controls both transmitter as well as receiver thus providing synchronization at bit level.

- (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.
- The major protocols used by the physical layer include Bluetooth, OTN (Optical Transport Network), DSL, IEEE.802.11, IEEE.802.3, and so on. Hub, Repeater, Modem, Cables etc., are physical layer connecting devices.

2. Data Link Layer:

- The 2nd layer of the OSI model is the data link layer. The goal of the data link layer is to provide reliable, efficient communication between adjacent machines connected by a single communication medium.
- Data link layer sends data frames from the Network layer to the Physical layer. The data link layer divides the stream of bits received from the network layer to manageable data units called frames.
- Data link layer is divided into following two sub layers:
 - (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. LLC sublayer provides interface between the media access methods.
- **Functions** of data link layer are given below:
 - (i) **Framing:** Framing provides a way for a sender to transmit a set of bits that are meaningful to the receiver. Data link layer performs various framing functions like frame traffic control, frame sequencing, frame delimiting, frame error checking and so on.
 - (ii) **Physical Addressing:** After creating frames, the data link layer adds physical addresses (MAC address) of sender and/or receiver in the header of each frame.
 - (iii) **Flow Control:** Flow control is the traffic regulatory mechanism implemented by a 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 decide 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.
- The protocols are used by the Data Link Layer includes Point-to-Point Protocol (PPP), Point-to-Point High-Level Data Link Control (HDLC), Serial Line Internet Protocol (SLIP), Spanning Tree Protocol (STP,) Address Resolution Protocol (ARP), IEEE.802.3, ARCNET etc. Switch and Bridge are data link layer connecting devices.

3. Network Layer:

- 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 network, network layer is responsible for delivery of data packets.
- **Functions** of network layer are given below:
 - (i) **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 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:** 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. Routes frames among networks.
 - (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.

- (v) **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.
- (vi) **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, network layer divides the large packets into fragments so that they can be easily sent on the physical medium.
- The network layer uses protocols such as Internet Protocol (IP), Internet Protocol version 4 (IPv4), Internet Protocol version 6 (IPv6), Internet Control Message Protocol (ICMP), Internet Group Management Protocol (IGMP), Internet Protocol Security (IPsec), Internetwork Packet Exchange (IPX), Routing Information Protocol (RIP) etc. Network layer uses networking connecting devices such as routers and gateway.
- 4. Transport Layer:**
- The 4th layer of the OSI model is the transport layer. Transport layer is responsible for the process to process delivery of the entire message. A process is an application program running on a host.
 - Transport layer ensures that packets are delivered error free, in sequence with no losses or duplications. Transport layer unpacks, reassembles and sends receipt of messages at the receiving end.
 - Transport layer provides flow control, error handling, and solves transmission problems. The transport layer is responsible for source-to-destination, (end-to-end) delivery of the entire message.
 - Transport layer provides following two types of services:
 - (i) In **Connection Oriented Transmission** the receiving device sends an acknowledgment, back to the source after a packet or group of packet is received. This type of transmission is also known as a reliable transport method. Because connection oriented transmission requires more packets to be sent across the network, it is considered a slower transmission method.
 - (ii) In **Connectionless Transmission** the receiver does not acknowledge receipt of a packet that the packet arrives just fine. This approach allows for much faster communication between devices.
 - **Functions** of transport layer are given below:
 - (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 the 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:

(April 17)

- The 5th 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.
- Session layer 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.
- **Function** of session layer are given below:
 - (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 or full duplex mode.

- (ii) **Dialog Separation or 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.
- (iii) **Session Establishment, Maintenance and Termination:** It allows two application processes on different machines to establish, use and terminate a connection, called a session.
- (iv) **Session Support:** It performs the functions that allow these processes to communicate over the network, performing security, name recognition, logging and so on.

- The protocols used in session layer includes Layer 2 Tunneling Protocol (L2TP), Point-to-Point Tunneling Protocol (PPTP), Network Basic Input Output System (NetBIOS), PAP (Password Authentication Protocol), Sockets Direct Protocol (SDP) etc.

6. Presentation Layer:

(April 17)

- The 6th layer of the OSI model is the presentation layer. The Presentation layer is also called 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.
 - **Functions** of presentation layer are given below:
 - (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.
 - The presentation layer uses protocols Multipurpose Internet Mail Extensions (MIME) Network News Transfer Protocol (NNTP), Transport Layer Security (TLS) and Secure Sockets Layer (SSL) etc.
- ## 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.

- Application layer 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.
- **Functions** of application layer are given below:
 - (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 (FTAM):** 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) **Remote Logins:** This layer allows logging into a host which is remote.
 - (v) **Directory Services:** This application provides distributed database sources and access for global information about various objects and services.
- Application layer uses protocols such as Secure Shell (SSH), File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), Simple Mail Transfer Protocol (SMTP), Internet Message Access Protocol (IMAP), Reverse Address Resolution Protocol (RARP), Bootstrap Protocol (BOOTP), Simple Network Management Protocol (SNMP), Border Gateway Protocol (BGP), Hypertext Transfer Protocol (HTTP) etc.

1.4.2 TCP/IP Reference Model

- TCP/IP stands for Transmission Control Protocol/Internet Protocol. The TCP/IP model was developed by the U.S. Department of Defense (DoD) to connect multiple networks and preserve data integrity.
- The TCP/IP is the conceptual model and set of communications protocols used on the Internet and similar computer networks.
- The TCP/IP protocol suite establishes the technical foundation of the Internet. TCP/IP protocol suite also called the Internet protocol suite.
- The TCP/IP is a protocol suite (a set of protocols organized in different layers) used in the Internet today. It is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality.
- The term hierarchical means that each upper level protocol is supported by the services provided by one or more lower level protocols.

- The original TCP/IP protocol suite was defined as four software layers built upon the hardware. Today, however, TCP/IP is thought of as a five-layer model as shown in Fig. 1.47.

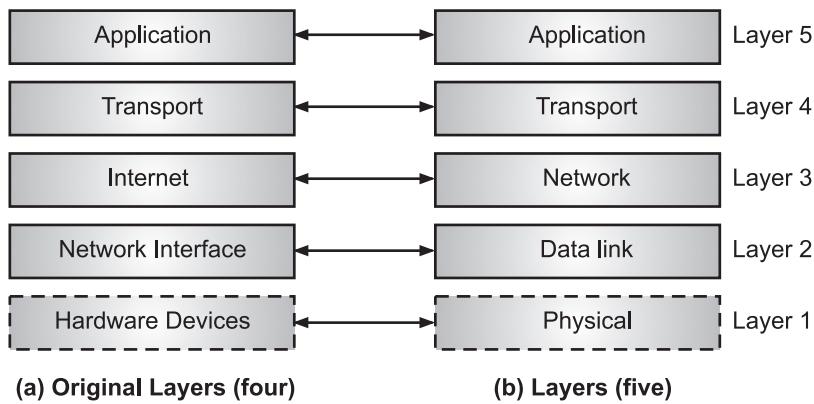


Fig. 1.47: Layers in the TCP/IP Protocol Suite

- Fig. 1.48 shows five-layer TCP/IP reference model.

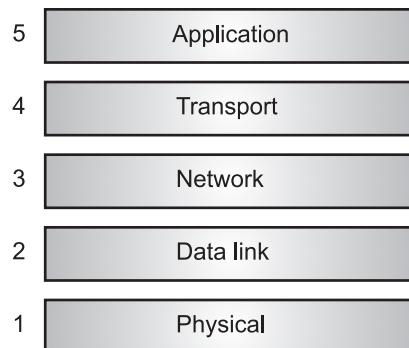


Fig. 1.48: Five Layers in the TCP/IP Reference Model

1.4.2.1 Layered Structure of TCP/IP

- TCP/IPs an industry-standard protocol suite for Wide Area Networks (WANs) developed in the 1970s and 1980s by the U.S. Department of Defense (DoD).
- TCP/IP is not one protocol, but is a suite of many protocols. The protocols define applications, transport controls, networking, routing, and network management.
- The TCP/IP is a set of protocols, or a protocol suite, that defines how all transmissions are exchanged across the Internet.
- TCP/IP protocol suite contains five layers. To better understand the duties of each layer, we need to think about the logical connections between layers.
- Fig. 1.49 shows logical connections in simple internet.

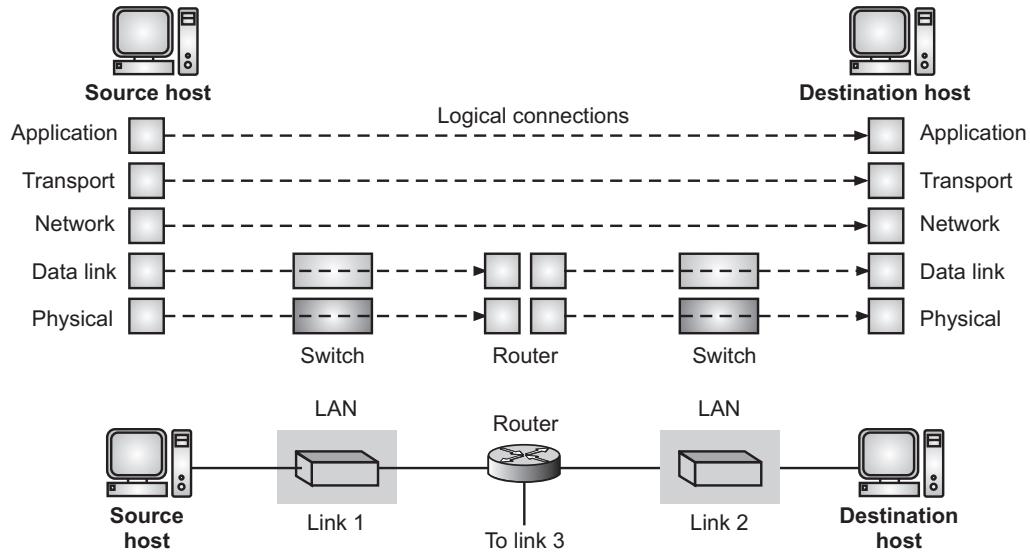


Fig. 1.49: Logical Connection between Layers of the TCP/IP Protocol Suite

- Using logical connections in TCP/IP protocol suite makes it easier for us to think about the duty of each layer.
- As the Fig. 1.49 shows the duty of the application, transport, and network layers is end-to-end.
- However, the duty of the data-link and physical layers is hop-to-hop, in which a hop is a host or router. In other words, the domain of duty of the top three layers is the internet, and the domain of duty of the two lower layers is the link.

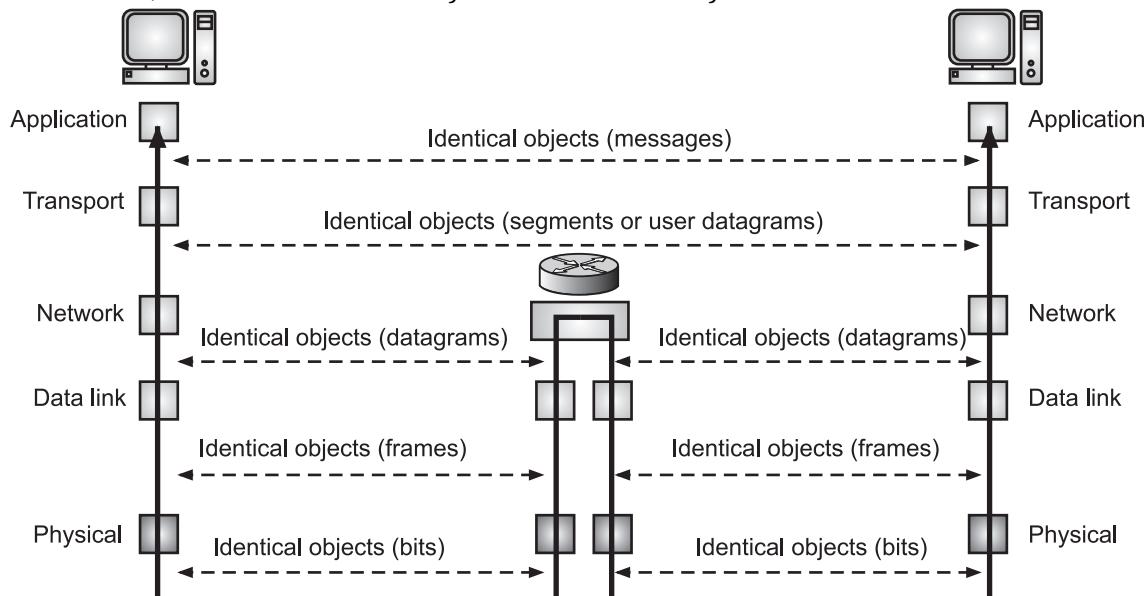


Fig. 1.50: Identical Objects in the TCP/IP Protocol Suite

- Another way of thinking of the logical connections in TCP/IP network-model is to think about the data unit created from each layer.
- In the top three layers, the data unit (packets) should not be changed by any router or link-layer switch.
- In the bottom two layers of TCP/IP protocol suite, the packet created by the host is changed only by the routers, not by the link-layer switches.
- Fig. 1.50 shows the identical objects below each layer related to each device.

1.4.2.2 Functions of Each Layer of TCP/IP Reference Model

- After understanding the concept of logical communication, we are ready to briefly discuss the duty/function of each layer in TCP/IP network model.

1. Physical Layer:

- The physical layer (lowest level) in TCP/IP network model is responsible for carrying individual bits in a frame across the link.
- The communication between two devices at the physical layer is still a logical communication because there is another, hidden layer, the transmission media, under the physical layer.
- Two devices are connected by a transmission medium (cable or air). We need to know that the transmission medium does not carry bits; it carries electrical or optical signals.
- So the bits received in a frame from the data-link layer are transformed and sent through the transmission media, but we can think that the logical unit between two physical layers in two devices is a bit.
- There are several protocols that transform a bit to a signal, including Ethernet, Token ring (820.3), FDDI, X.25, Frame relay.

2. Data Link Layer:

- An internet is made up of several links (LANs and WANs) connected by routers. There may be several overlapping sets of links that a datagram can travel from the host to the destination. The routers are responsible for choosing the best links.
- However, when the next link to travel is determined by the router, the data-link layer in TCP/IP protocol suite is responsible for taking the datagram and moving it across the link.
- The link can be a wired LAN with a link-layer switch, a wireless LAN, a wired WAN, or a wireless WAN.
- We can also have different protocols used with any link type. In each case, the data-link layer is responsible for moving the packet through the link.
- TCP/IP does not define any specific protocol for the data-link layer. It supports all the standard and proprietary protocols.

- Any protocol that can take the datagram and carry it through the link suffices for the network layer. The data-link layer takes a data-gram and encapsulates it in a packet called a frame.
- Each link-layer protocol may provide a different service. Some link-layer protocols provide complete error detection and correction, some provide only error correction.
- Examples of data-link layer protocols are Ethernet, IEEE 802.2 framing and Point-to-Point Protocol (PPP) framing.

3. Network Layer:

- The network layer in TCP/IP protocol suite is responsible for creating a connection between the source computer and the destination computer. The communication at the network layer is host-to-host.
- However, since there can be several routers from the source to the destination, the routers in the path are responsible for choosing the best route for each packet.
- The network layer is responsible for host-to-host communication and routing the packet through possible routes.
- The network layer in the Internet includes the main protocol Internet Protocol (IP), that defines the format of the packet, called a datagram at the network layer. IP also defines the format and the structure of addresses used in network layers.
- IP is also responsible for routing a packet from its source to its destination, which is achieved by each router forwarding the datagram to the next router in its path.
- IP is a connectionless protocol that provides no flow control, no error control, and no congestion control services.
- The network layer in TCP/IP protocol suite also has some auxiliary protocols that help IP in its delivery and routing tasks. Some of them are:
 - (i) The **Internet Control Message Protocol (ICMP)** helps IP to report some problems when routing a packet.
 - (ii) The **Internet Group Management Protocol (IGMP)** helps IP in multitasking.
 - (iii) The **Dynamic Host Configuration Protocol (DHCP)** helps IP to get the network-layer address for a host.
 - (iv) The **Address Resolution Protocol (ARP)** helps IP to find the link-layer address of a host or a router when its network-layer address is given.

4. Transport Layer:

- The logical connection at the transport layer in TCP/IP protocol suite is also end-to-end. The transport layer at the source host gets the message from the application layer, encapsulates it in a transport-layer packet (called a segment or a user datagram in different protocols) and sends it, through the logical (imaginary) connection, to the transport layer at the destination host.

- In other words, the transport layer in TCP/IP protocol suite is responsible for giving services to the application layer, to get a message from an application program running on the source host and deliver it to the corresponding application program on the destination host.
- There are a few transport layer protocols in the Internet, each designed for some specific task. The main protocol of transport layer is Transmission Control Protocol (TCP).
- TCP is a connection-oriented protocol that first establishes a logical connection between transport layers at two hosts before transferring data. TCP creates a logical pipe between two TCPs for transferring a stream of bytes.
- TCP provides flow control (matching the sending data rate of the source host with the receiving data rate of the destination host to prevent overwhelming the destination), error control (to guarantee that the segments arrive at the destination without error and resending the corrupted ones), and congestion control to reduce the loss of segments due to congestion in the network.
- The other common transport layer protocol is User Datagram Protocol (UDP), UDP is a connectionless protocol that transmits user datagrams without first creating a logical connection.
- In UDP, each user datagram is an independent entity without being related to the previous or the next one (the meaning of the term connectionless).
- UDP is a simple protocol that does not provide flow, error, or congestion control. UDP's simplicity, which means small overhead, is attractive to an application program that needs to send short messages and cannot afford the retransmission of the packets involved in TCP, when a packet is corrupted or lost.
- A new protocol, Stream Control Transmission Protocol (SCTP) is designed to respond to new applications that are emerging in the multimedia.

5. Application Layer:

- Fig. 1.49 shows the logical connection between the two application layers is end-to-end. The two application layers' exchange messages between each other as though there were a bridge between the two layers. However, we should know that the communication is done through all the layers.
- Communication at the application layer is between two processes (two programs running at this layer). To communicate, a process sends a request to the other process and receives a response.
- Process-to-process communication is the duty of the application layer. The application layer in the Internet includes many predefined protocols, but a user can also create a pair of processes to be run at the two hosts.

- The HyperText Transfer Protocol (HTTP) is a vehicle for accessing the World Wide Web (WWW or Web). The Simple Mail Transfer Protocol (SMTP) is the main protocol used in electronic mail (e-mail) service.
- The File Transfer Protocol (FTP) is used for transferring files from one host to another. The Terminal Network (TELNET) and Secure Shell (SSH) are used for accessing a site remotely.
- The Simple Network Management Protocol (SNMP) is used by an administrator to manage the Internet at global and local levels.
- The Domain Name System (DNS) is used by other protocols to find the network-layer address of a computer. The Internet Group Management Protocol (IGMP) is used to collect membership in a group.

1.4.3 Comparison of OSI and TCP/IP Models

(Oct. 17, 18; April 18, 19)

- Following table compare OSI reference model and TCP/IP model:

Sr. No.	OSI Reference Model	TCP/IP Model
1.	OSI refers to Open Systems Interconnection.	TCP refers to Transmission Control Protocol/ Internet Protocol.
2.	OSI model had Seven (7) layers.	TCP/IP model has five (5) layers.
3.	OSI is less reliable.	TCP/IP is more reliable.
4.	Developed by ISO (International Standard Organization).	Developed by the Department of Defense (DoD).
5.	OSI is a conceptual model.	TCP/IP is a client-server model, i.e. when the client requests for service it is provided by the server.
6.	Protocol independent standard.	Protocol dependent standard.
7.	OSI follows a horizontal approach.	TCP/IP follows a vertical approach.
8.	OSI model follows a bottom-up approach.	TCP/IP follows a top-bottom approach.
9.	In the OSI model, model was developed before the development of protocols.	In the TCP/IP model, protocol were developed first and then the model was developed.
10.	Model describes any type of network.	Model only describes TCP/IP which is not useful for describing any other networks.

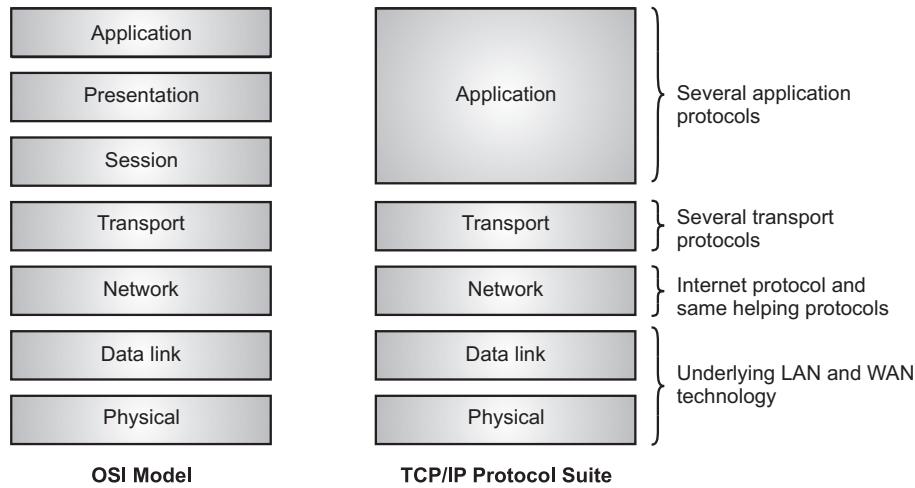


Fig. 1.51: Comparison Diagram for ISO-OSI and TCP/IP Network Reference/Models

1.4.4 Connection Devices in different Layers

(April 17, Oct. 18)

- Computer network connecting devices are physical devices which are required for communication and interaction between devices on a computer network.
- The network devices are playing an important role in network communication, each device has a different role.

Network Connecting Devices for OSI Model:

- Fig. 1.52 shows positions of network devices in OSI model.

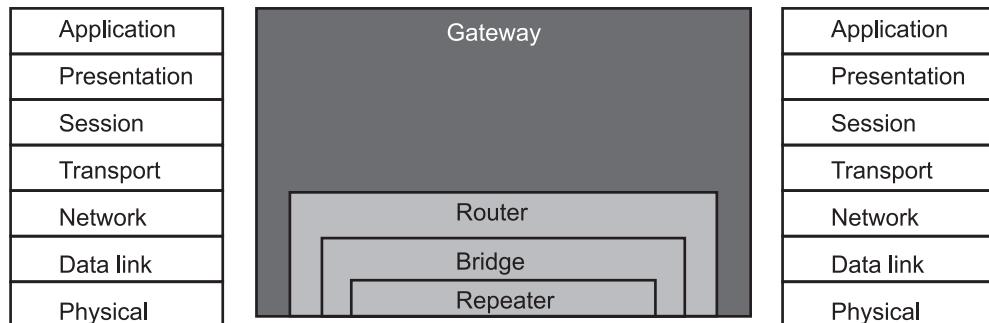


Fig. 1.52: OSI Model and Position of Networking Devices

- Hardware devices that are used to connect computers, printers, fax machines and other electronic devices to a network are called network devices.
- Without network devices a computer network cannot be made and work. Following are the list of network devices shows their need and importance in networking:
 1. **Hub:** Hub is important because it broadcasts data from one port to all other ports in the network. A hub works on the physical layer (Layer 1) of the OSI model. Hubs are available with 4, 8, 12, 24, 48 ports. A hub is a networking device which

- receives signal from the source, amplifies it and sends it to multiple destinations or computers.
2. **Switch:** It is used in to send data point to point, meaning directly from one computer to another through a switch. Network switch is a small hardware device that joins multiple computers together within one Local Area Network (LAN). Network switches operate at layer two (Data Link Layer) of the OSI model. A network switch can be defined as the device that connects the network devices or network segments. Switches available with 4, 8, 12, 24, 48, 64 ports.
 3. **Repeater:** The repeaters are used in places where amplification of input signal is necessary. A repeater (or regenerator) is an electronic device that operates on a physical layer of the OSI model. A repeater is an electronic device that receives a signal and retransmits it. Repeaters are used to extend transmissions so that the signal can cover longer distances.
 4. **Router:** A router is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet. A router operates in the Network, Data link, and Physical layers of the OSI model.
 5. **Gateway:** Needed when two different network technologies are being used. Gateway acts as translator switch-intelligent device which sends data to a particular port. Gateway works on all seven (7) layers of the OSI model. Gateway is a network device used to connect two or more dissimilar networks. In networking parlance, networks that use different protocols are dissimilar networks.
 6. **Bridge:** A network bridge is a computer networking device that creates a single aggregate network from multiple communication networks or network segments. This function is called network bridging. Bridging is distinct from routing. Routing allows multiple networks to communicate independently and yet remain separate, whereas bridging connects two separate networks as if they were a single network. It works at the Data Link layer of the OSI Model and connects the different networks together and develops communication between them. If one or more segments of the bridged network are wireless, the device is known as a wireless bridge.
 7. **Modem:** Modem is a device that enables a computer to send or receive data over telephone or cable lines. The modem works at the Physical Layer of the OSI model. The main function of the modem is to convert digital signals into analog and vice versa. Modem is a combination of two devices – modulator and demodulator. The modulator converts digital data into analog data when the data is being sent by the computer. The demodulator converts analog data signals into digital data when it is being received by the computer.

Network Connecting Devices for TCP/IP Model:

- The TCP/IP model is based on a five-layer model for networking.
- Physical layer of TCP/IP model is responsible for physical connectivity of two devices. Some of the devices used in Physical layer are, Ethernet, Hub, Repeaters etc.
- The devices used in the Data link layer of TCP/IP model are Bridges, Modem, Network Interface Cards (NICs) etc.
- The devices used in the Network layer of TCP/IP model are Router, Brouter etc. The devices used in transport layer of TCP/IP model are Gateway, Firewall etc.
- The devices used in the Application layer of TCP/IP model are Phones, Servers, Gateways etc.

PRACTICE QUESTIONS**Q.I Multiple Choice Questions:**

1. Which refers to the exchange of data between two devices through some form of wired or wireless transmission media?

(a) Data communication	(b) Networking
(c) Data transfer	(d) None of these
2. Which is an interconnection of computers and computing equipment using either wires or radio waves and can share data and computing resources?

(a) Data Communication	(b) Computer Network
(c) Data Transmission	(d) None of these
3. Which means the transfer of information between humans, computers or machines in a meaningful way?

(a) Communication	(b) Networking
(c) Data exchange	(d) None of these
4. A network of networks is called an _____.

(a) Internetwork	(b) Internet
(c) Both (a) and (b)	(d) None of these
5. Components of data communication includes _____.

(a) Sender and Message	(b) Protocol and Receiver
(c) Transmission Medium	(d) All of these
6. Which plays an important role in networking?

(a) Data	(b) Protocol
(c) Message	(d) All of these
7. Data can be represented as _____.

(a) Text and Numbers	(b) Audio and Video
(c) Images/Graphics	(d) All of these

8. In which mode, the communication can take place in both directions, but only in one direction at a time.
 - (a) Simplex
 - (b) Full-duplex
 - (c) Half-duplex
 - (d) All of these
9. Which is an interconnected collection of autonomous computers?
 - (a) Protocol
 - (b) Network
 - (c) Communication
 - (d) All of these
10. Network criteria includes _____.
 - (a) Performance
 - (b) Reliability
 - (c) Type of communication media
 - (d) All of these
11. Connection between two directly interconnected devices/nodes is referred to as _____ connection.
 - (a) Multipoint
 - (b) Point-to-point
 - (c) Broadcast
 - (d) All of these
12. Which refers to the way in which a network is laid out physically?
 - (a) Protocol
 - (b) Message
 - (c) Topology
 - (d) None of these
13. In which topology all nodes are connected to a central cable?
 - (a) Star
 - (b) Bus
 - (c) Topology
 - (d) None of these
14. Which is a privately-owned network covering a small geographical area, (less than 1 km) like a home, office etc.
 - (a) WAN
 - (b) MAN
 - (c) LAN
 - (d) All of these
15. Which is a combination of several point-to-point WANs that are connected by switches.
 - (a) Point-to-point WAN
 - (b) Switched WAN
 - (c) Multipoint MAN
 - (d) All of these
16. A _____ needs to forward data from a network to another network when required.
 - (a) Switch
 - (b) Hub
 - (c) Gateway
 - (d) Router
17. In which network, a dedicated connection, (called a circuit) is always available between the two end systems.
 - (a) Packet switched
 - (b) Message switched
 - (c) Circuit switched
 - (d) None of these

ANSWERS

1. (a)	2. (b)	3. (a)	4. (c)	5. (d)	6. (a)	7. (d)
8. (c)	9. (b)	10.(d)	11. (b)	12. (c)	13. (b)	14. (c)
15. (b)	16. (a)	17. (c)	18. (a)	19. (d)	20. (c)	21. (b)
22. (d)	23. (c)	24. (b)				

Q. II Fill in the Blanks:

1. A system of interconnected computers and computerized peripherals such as printers is called computer ____.
 2. ____ is the process of establishing connection or link between two entities for the transfer/exchange of information.

3. The interconnected computers can share resources, which called _____.
4. The network _____ consists of instruction sets, that make possible the services that we expect from a network.
5. _____ communication is the exchange of information between two computers capable of generating processing and interpreting data.
6. The meaningful, logical and processed data is called as _____.
7. The _____ is the information (data) to be communicated.
8. A _____ is a set of rules that governs data communications.
9. In _____ mode, the communication can take place in both directions simultaneously.
10. _____ enables its users to share and access enormous amount of information worldwide.
11. A set of layers and protocols is called a network _____.
12. A _____ network is a set of devices connected by channels on links and provides a service between users located at various geographical points.
13. Connection between two directly interconnected devices/nodes is referred to as _____ connection.
14. In _____ topology each device has a dedicated point-to-point link on it to a central controller, usually called hub or switch.
15. In ring topology, the computers in the network are connected in a circular fashion which form of a _____.
16. _____ are widely used to connect personal computers and workstations to share resources (printers, scanners) and exchange information.
17. A _____ is a computer network that interconnects users with computer resources in a geographic region of the size of a metropolitan area like entire city.
18. _____ oriented services are similar to telephone systems which are highly reliable.
19. The connection of two or more networks is called _____ or Internet.
20. _____ is an organization offering access to internet with monthly/yearly fee.
21. Digital Subscriber Line (DSL) provides Internet access by transmitting digital data over the wires of a local _____ network.
22. In _____ connection, computer uses its modem to dial a telephone number given to the user by an Internet Service Provider.
23. A communication system designed in such a manner is referred to as _____ architecture.
24. The _____ model is a layered framework for the design of network systems that allows communication between all types of computer system.

25. The _____ is the conceptual model and set of communications protocols used on the Internet and similar computer networks.

ANSWERS

1. Network	2. Communication	3. Networking	4. Software
5. Data	6. Information	7. Message	8. Protocol
9. Full-duplex	10. Internet	11. Architecture	12. Communication
13. Point-to-point	14. Star	15. Ring	16. LANs
17. MAN	18. Connection	19. Internetworks	20. Internet Service Provider (ISP)
21. Telephone	22. Dial-up	23. Layered	24. OSI
25. TCP/IP			

Q. III State True or False:

1. The process of sending or receiving data between two points/entities of a computer networks is known as data communication.
2. A network is a set of devices (sometimes called nodes or stations) interconnected by media links.
3. A data communication network is a collection of two or more computing devices that are interconnected to enable them to share data.
4. A computer network is a set of electronically connected computers which can share information and resources among themselves.
5. The hardware consists of the physical equipment that carries signals from one point to the network to another.
6. A computer network is an interconnection of computers and computing equipment using either wires or radio waves over small or large geographic area.
7. The term topology refers to the way a network is laid out, either physically or logically.
8. Internet is computer based global information system which composed with number of interconnected computer networks.
9. A data communication system has five components namely sender, message, receiver, transmission medium, and protocol.
10. In reference model a layer is a grouping of related tasks involving the transfer of information.
11. In full-duplex mode, the communication can take place in only one direction.
12. Computer network is divided in to wired and wireless network.
13. In point-to-point connection, a single link is shared by multiple devices.

14. 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.
15. A WAN is a geographically-dispersed collection of LANs.
16. The switched WAN connects the end systems.
17. An internetwork is a collection of individual networks, connected by intermediate networking devices, that functions as a single large network.
18. In a computer network, the communication between the two ends is done in blocks of data known as packets.
19. The Internet is the global system of interconnected computer networks that uses the Internet protocol suite (TCP/IP) to communicate between networks and devices.
20. A cable modem can be added to or integrated with a set-top box that provides the TV set for Internet access.
21. The entities comprising the corresponding layers on different machines are called peers.
22. A network consists of a series of levels called layers.
23. TCP/IP stands for Transmission Control Protocol/Internet Protocol.
24. Connection-oriented service is modeled after the postal system. In this type of services, no connection is established between source and destination.
25. The seven layers of OSI model are physical layer, data link layer, network layer, transport layer, session layer, presentation layer and application layer.
26. TCP/IP protocol suite also called as Internet protocol suite.
27. The original TCP/IP protocol suite was defined as four software layers built upon the hardware. Today, however, TCP/IP is thought of as a five-layer model.
28. Data in networking can be available in the form of text, number, images, audio and video.
29. Internet is a world-wide global system of interconnected computer networks.
30. Networking hardware is designed to help set up, manage, and/or monitor computer networks.

ANSWERS

1. (T)	2. (T)	3. (T)	4. (T)	5. (T)	6. (T)
7. (T)	8. (T)	9. (T)	10. (T)	11. (F)	12. (T)
13. (F)	14. (T)	15. (T)	16. (T)	17. (T)	18. (T)
19. (T)	20. (T)	21. (T)	22. (T)	23. (T)	24. (F)
25. (T)	26. (T)	27. (T)	28. (T)	29. (T)	30. (F)

Q. IV Answer the following Questions:**(A) Short Answer Questions:**

1. What is data communication?
2. List components of data communication.
3. What is network?
4. Define the term computer network.
5. Define LAN.
6. What is WAN?
7. List design issues of the layer.
8. Give function of network software.
9. Define switching.
10. What is protocol?
11. Explain purpose of reference model.
12. Define the term internet.
13. List layers of OSI model.
14. Define MAN.
15. What is topology?
16. What is meant by data representation?
17. List layers of TCP/IP model.
18. Which methods are used for accessing Internet.
19. State any two characteristics of data communication.
20. What network hardware?
21. List network devices for TCP/IP model.
22. What are the types of computer network?

(B) Long Answer Questions:

1. With the help of diagram describe components of data communication.
2. Explain computer network diagrammatically.
3. What is data and information? Define and compare them.
4. Describe modes in data communication with advantages and disadvantages.
5. Explain network criteria in detail.
6. Describe point-to-point and multipoint connections in detail.
7. Define topology. List types of topologies.
8. Describe the following topologies with their advantages and disadvantages:
 - (i) Bus
 - (ii) Tree

- (iii) Mesh
 - (iv) Star
 - (v) Ring.
9. Compare LAN, MAN and WAN.
 10. Explain point-to-point WAN and switched WAN with diagram.
 11. What is circuit switched network? Explain in detail.
 12. Define internet? Enlist ways for accessing internet.
 13. Explain protocol hierarchies in detail.
 14. Describe design issues of layers in detail.
 15. With the help of diagram describe connection-oriented and connection-less services.
 16. Describe OSI model with its layers. Also explain functions of each layer.
 17. Explain TCP/IP OSI model with its layers. Also explain functions of each layer.
 18. Differentiate between OSI and TCP/IP models.

UNIVERSITY QUESTIONS AND ANSWERS

April 2016

1. Give diagrammatic representation of bus and mesh topology. **[1 M]**
- Ans.** Refer to Sections 1.2.4.2.2 and 1.2.4.2.4.
2. What are the advantages of point-to-point network? **[2 M]**
- Ans.** Refer to Section 1.2.4.1, Point (1).
3. What is internetworking? **[1 M]**
- Ans.** Refer to Section 1.2.5.4.

April 2017

1. Define protocol with its key elements. **[1 M]**
- Ans.** Refer to Section 1.1.2, Point (4).
2. Define mesh topology. **[1 M]**
- Ans.** Refer to Section 1.2.4.2.4.
3. Which devices operate at physical layer? **[1 M]**
- Ans.** Refer to Section 1.4.4.
4. State the difference between LAN and WAN. **[5 M]**
- Ans.** Refer to Page No. 1.29 and 1.30.
5. What are the responsibilities of session and presentation layer? **[5 M]**
- Ans.** Refer to Section 1.4.1.2, Points (5) and (6).

6. Explain star topology with their advantages. [2 M]

Ans. Refer to Section 1.2.4.2.1.

October 2017

1. List two similarities between TCP/IP and OSI model. [1 M]

Ans. Refer to Section 1.4.3.

2. For n devices in a network, what is the number of cables required for ring topology? [1 M]

Ans. Refer to Section 1.2.4.2.3.

3. Explain the OSI reference model in detail. [5 M]

Ans. Refer to Section 1.4.1.

4. Write in detail about simplex, half duplex and full duplex data communication. [5 M]

Ans. Refer to Section 1.1.4.

April 2018

1. Write any two advantages of star topology. [1 M]

Ans. Refer to Section 1.2.4.2.1.

2. What is the responsibility of physical layer. [1 M]

Ans. Refer to Section 1.4.1.2, Point (1).

3. Give the diagrammatic representation of mesh topology. [1 M]

Ans. Refer to Sections 1.2.4.2.4.

4. What is topology? Explain the ring topology with advantages and disadvantages. [5 M]

Ans. Refer to Sections 1.2.4.2 and 1.2.4.2.3.

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

Ans. Refer to Section 1.4.3.

October 2018

1. Define protocols. What are its key elements? [1 M]

Ans. Refer to Section 1.1.2, Point (4).

2. Which topology requires a multipoint connection? [1 M]

Ans. Refer to Section 1.2.4.2.

3. Which device operates in physical layer? [1 M]

Ans. Refer to Section 1.4.4.

4. Explain similarities and differences between OSI and TCP/IP reference models. [5 M]

Ans. Refer to Section 1.4.3.

5. State advantages and disadvantages of star topology.

[2 M]

Ans. Refer to Section 1.2.4.2.1.

April 2019

1. Write disadvantages of star topology.

[1 M]

Ans. Refer to Section 1.2.4.2.1.

2. List any four application layer protocols.

[1 M]

Ans. Refer to Section 1.4.1.2, Point (7).

3. What is computer network?

[1 M]

Ans. Refer to Section 1.2.1.

4. Compare and contrast OSI and TCP/IP model.

[5 M]

Ans. Refer to Section 1.4.3.

5. State advantages and disadvantages of mesh topology.

[2 M]

Ans. Refer to Section 1.2.4.2.4.



Lower Layers

Objectives...

- To understand Lower Layers (Physical and Data Link)
- To learn Design Issues and Services of Data Link Layer
- To study Framing Methods Channel Allocation Problem with its Methods
- To understand Switching and its various Techniques
- To study Wired LAN and Wireless LAN

2.0 INTRODUCTION

(April 18)

- The physical layer (layer 1) and data link layer (layer 2) are the lower layers of the OSI model. The physical layer defines the physical characteristics and functions of the physical devices and interfaces so that transmission can occur.
- The data link layer is responsible for the reliable transfer of data frames from one node to another connected by the physical layer.
- The physical layer is concerned with transmission of raw bits over a communication channel/medium.
- The physical layer 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.
- To be transmitted, data must be transformed to electromagnetic signals. It is the layer which actually interacts with transmission media, which connects network components together.
- The physical layer 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. Physical layer does that.
- The data link layer is the second lower 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.

2.1 COMMUNICATION AT THE PHYSICAL LAYER

- The physical layer (layer 1) of OSI and TCP/IP models deals with transmission of individual bits from one node to another over a physical medium.
- Communication at the physical layer means exchanging signals. Signal is an electrical, electronic or optical representation of data, which can be sent over a communication medium.
- Data is transmitted from one point or entity to another point or entity by means of electrical signals that may be in digital and analog form.
- 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 data comes in a variety of forms such as text, graphics, audio, video and animation.
- Signals can be either analog or digital. Analog signals have infinite values in a range and Digital signals have a limited number of defined values.
- Analog signals are used to represent analog data, and digital signals are used to represent digital data.
- Data can be analog or digital. Analog data refers to information that is continuous. For example, sounds made by a human voice generate continuous waves in the air.
- Digital data refers to information that has discrete states. Digital data takes on discrete values. For example, data is stored in computer memory in the form of 0s and 1s.
- The purpose of the physical layer is to create the electrical, optical, or microwave signal that represents the bits in each frame. These signals are then sent on the media one at a time.

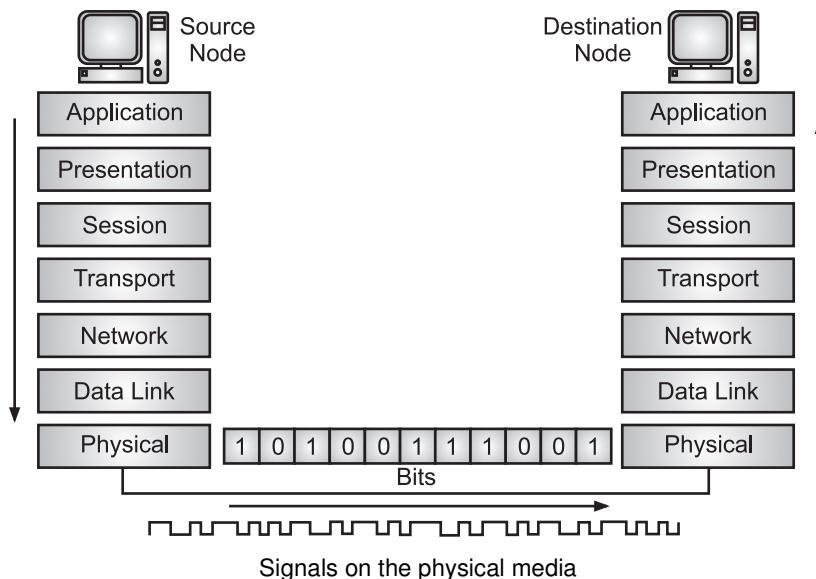


Fig. 2.1: Communication at the Physical Layer of OSI Model

- It is also the job of the physical layer to retrieve these individual signals from the media, restore them to their bit representations, and pass the bits up to the data link layer as a complete frame.
- The OSI physical layer provides the means to transport across the network media the bits that make up a data link layer frame.
- The physical layer accepts a complete frame from the data link layer and encodes it as a series of signals that are transmitted onto the local media.

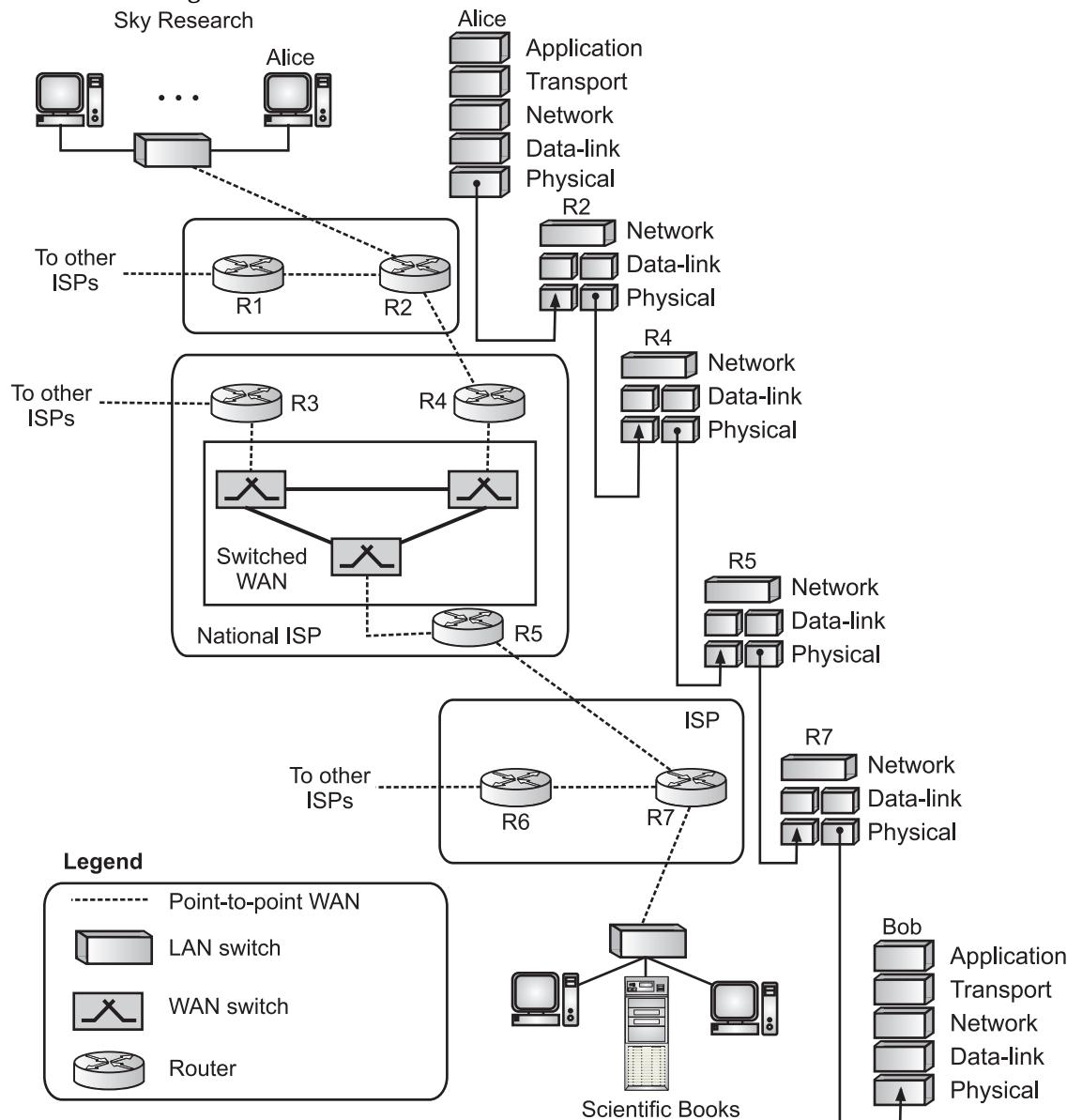


Fig. 2.2: Communication at the Physical Layer of TCP/IP Model

2.1.1 Data Rate Limits

(April 16, 19, Oct. 18)

- 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:
 - The bandwidth available,
 - The level of the signals we use, and
 - 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: one by Nyquist for a noiseless channel, another by Shannon for a noisy channel.

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 1: Consider a noiseless channel with a band width of 4000 Hz transmitting a signal with two signal levels. What will be the maximum bit rate?

Solution:

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

Example 2: We need to send 265 kbps over a noiseless channel with a bandwidth of 20 kHz. How many signal levels do we need?

Solution:

$$\begin{aligned}\text{Bit Rate} &= 2 \times \text{bandwidth} \times \log_2 L \\ 265,000 &= 2 \times 20,000 \times \log_2 L \\ \log_2 L &= 6.625 \\ L &= 2^{6.625} \\ L &= 98.7 \text{ levels}\end{aligned}$$

Example 3: 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:

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

Shannon's Law for Noisy Channel:

(Oct. 17)

- 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.

$$\text{Capacity} = \text{Bandwidth} \times \log_2 (1 + \text{SNR})$$

- 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 4: 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.

$$\begin{aligned}\text{Solution: } C &= B \log_2 (1 + \text{SNR}) \\ &= 3000 \log_2 (1 + 3162) \\ &= 3000 \log_2 3163 \\ &= 3000 \times 11.62\end{aligned}$$

$$\text{Capacity} = 341860 \text{ bps}$$

Example 5: 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.

$$\begin{aligned}C &= 2B \log_2(L), \\ 160 \times 10^3 &= 2 \times 20 \times 10^3 \log_2(L) \\ \log_2(L) &= 4 \\ L &= 2^4, \text{ which means 4 bits/baud.}\end{aligned}$$

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

$$\begin{aligned} C &= B \log_2(1 + S/N), \\ 160 \times 10^3 &= 20 \times 10^3 \log_2(1 + S/N) \\ \log_2(1 + S/N) &= 8 \\ S/N &= 2^8 - 1 \\ S/N &= 255 \\ S/N &= 24.07 \text{ dB.} \end{aligned}$$

Example 6: 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?

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

So,

$$\begin{aligned} 20 \times 10^6 &= 3 \times 10^6 \log_2(1 + SNR) \\ \log_2(1 + SNR) &= 20 / 3 = 6.667 \\ 1 + SNR &= 102 \\ \text{Hence, } SNR &= 101 \end{aligned}$$

Example 7: What is the channel capacity for a tele-printer channel with a 300 Hz bandwidth and a signal-to-noise ratio of 3 DB?

Solution:

Using Shannon's equation: $C = B \log_2(1 + SNR)$

We have $B = 300 \text{ Hz}$ and $SNR (\text{in dB}) = 3$,

Therefore, $SNR = 10^{0.3}$

$$\begin{aligned} C &= 300 \log_2(1 + 100.3) \\ C &= 300 \log_2(2.995) \\ C &= 474 \text{ bps} \end{aligned}$$

2.1.2 Performance of Network

- One important issue in networking is the performance of the network. Performance of the network depends upon several factors like Bandwidth, Throughput, Latency (delay), Bandwidth-delay product and Jitter.

2.1.2.1 Bandwidth

- In computer networks, the term bandwidth refers to the speed of data transmissions. It is a measure of the data that can be transmitted from one point to another in a given amount of time.
- To measure network performance, the one characteristic is bandwidth. In networking, we use the term bandwidth in two contexts with following two different measuring values:
 1. **Bandwidth in Hertz (Hz):** Bandwidth in hertz refers to the range of frequencies in a composite signal or the range of frequencies that the channel can pass. For example, the bandwidth of a subscriber telephone line is 4kHz.
 2. **Bandwidth in bits per second (bps):** Bandwidth in bits per second refers to the speed of bit transmission in a channel or link. For example, the bandwidth of a Fast Ethernet network or the links is a maximum of 100 Mbps means this network can send 100 Mbps.
- 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.

2.1.2.2 Throughput

- The throughput is a measure of how fast we can actually send data through a network. Throughput is the rate of successful message delivery over a communication channel/medium.
- Bandwidth in bits per second and throughput seems to be the 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 8: 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: Throughput is the amount of data moved successfully from one place to another place. That is 12,000 frames per minute and each Frame is carrying 10,000 bits.

$$\begin{aligned}\text{Throughput} &= \frac{12,000 \times 10,000}{60} \\ &= 2 \times 1000000 \text{ bits/seconds} \\ &= 2 \text{Mbps}\end{aligned}$$

2.1.2.3 Latency

(April 17)

- 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 is the time it takes for a packet to get across the network, from source to destination.

$$\text{Latency} = \text{Propagation time} + \text{Transmission time} + \text{Queuing time} + \text{Processing delay}$$

Propagation Time:

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

$$\text{Propagation time} = \frac{\text{Distance between Two Points}}{\text{Propagation speed}}$$

Example 9: 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: We calculate the propagation time as,

$$\begin{aligned}\text{Propagation time} &= \frac{12,000 \times 1000}{2.4 \times 10^8} \\ &= 50 \text{ ms}\end{aligned}$$

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 10: 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: Propagation time = $\frac{12000 \times 1000}{2.4 \times 10^8} = 50 \text{ ms}$

Transmission Time = $\frac{2500 \times 8}{10^9} = 0.020 \text{ ms}$

Queuing Time:

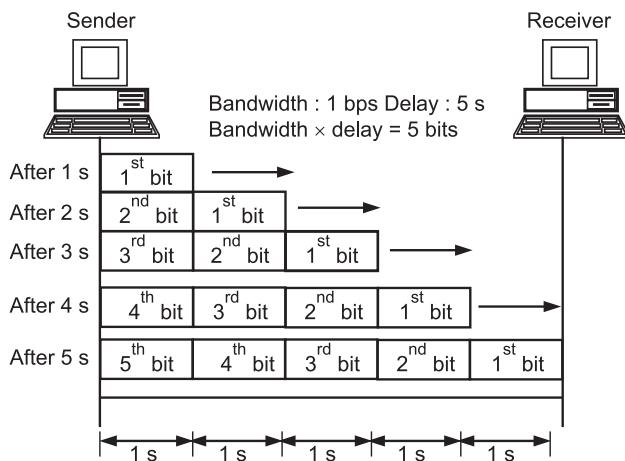
- The third component in latency is the queuing time, the time needed for each intermediate or end device to hold the message before it can be processed.
- The queuing time is not fixed; it depends upon the load on the network. When there is heavy traffic on the network, the queuing time increases.

2.1.2.4 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.
- The bandwidth-delay product defines the number of bits that can fill the network link. It gives the maximum amount of data that can be transmitted by the sender at a given time before waiting for acknowledgment.
- 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. 2.3 we can say that the bandwidth delay product is 1×5 , which 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. 2.3: Filling the Link with Bits for Case 1****Case 2:**

- Now, assume we have a bandwidth of 4bps. Fig. 2.4 shows there can be $4 \times 5 = 20$ bits on the line. At each second, there are 4 bits on the line, the duration of each bit is 0.25s.

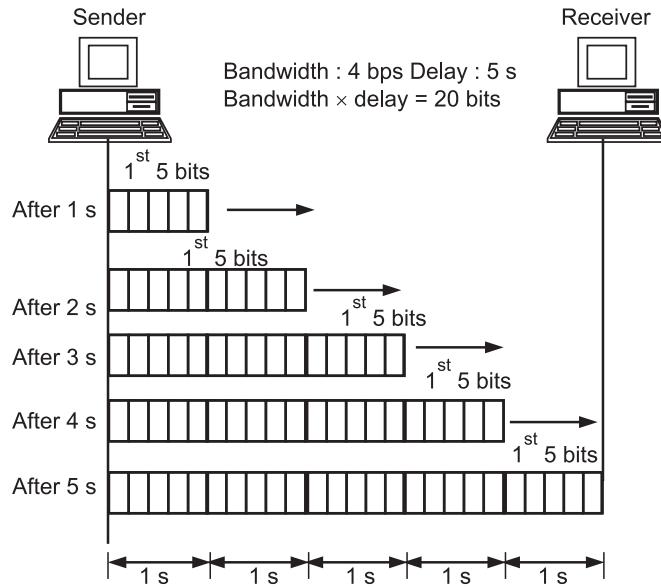
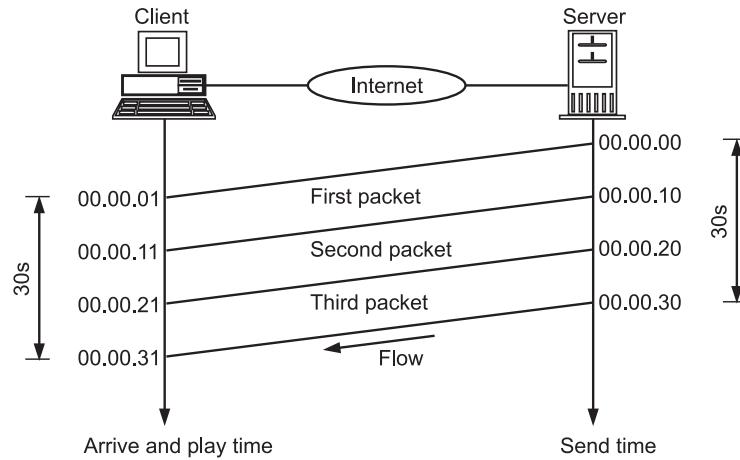


Fig. 2.4: Filling the Link with Bits in Case 2

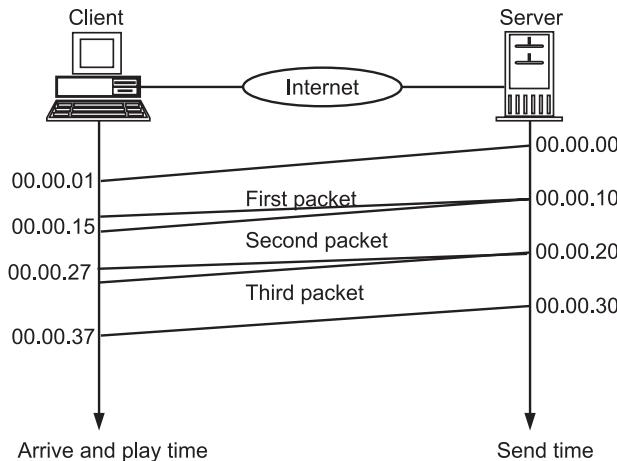
- The above two cases show that the product of bandwidth and delay is the number of bits that can fill the link.

2.1.2.5 Jitter

- Another performance issue that is related to delay is jitter. Jitter is the variance in time delay in milliseconds (ms) between data packets over a network. It is a disruption in the normal sequence of sending data packets.
- In technical terms, jitter is a “packet delay variance”. The jitter is considered as a problem when different packets of data face different delays in a network and the data at the receiver application is time-sensitive, i.e. audio or video data.
- 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 a client. Every packet contains 10 sec 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. 2.5 shows this idea.

**Fig. 2.5: Noise**

- 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. 2.6.

**Fig. 2.6: Jitter**

2.2 DATA LINK LAYER

- The data link layer is layer number 2 in the ISO-OSI and TCP/IP model. The data link provides for the transfer of data frames between hosts connected to the physical link.

- Data link layer transforms the physical layer, a raw transmission facility to a reliable link. It is responsible for moving frames from one hop (node) to the next i.e. hop-to-hop delivery.
- The data link layer takes services from the Physical layer and gives services to the network layer. Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver.
- Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
- The data link layer converts the raw transmission facility provided by the physical layer to a reliable and error-free link.
- The flow control function of data link layer coordinates that amount of data that can be sent before receiving acknowledgement.
- The data link layer also supports access control function. When a single communication channel is shared by multiple devices, the MAC sub-layer of the data link layer helps to determine which device has control over the channel at a given time.
- 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.

2.2.1 Design Issues

- The data-link layer is located between the physical and the network layers. The data link layer provides services to the network layer; it receives services from the physical layer.
- The design issues of the data link layer directly deal with its functionality and services. The main functions of the data link layer are:
 1. Controlling over the flow of data.
 2. Providing the service interface to the network layer.
 3. Dealing with the transmission errors.
- To do the above functions, the data link layer takes packets from the network layer and converts them to frames for transmission.
- The data link layer divides the stream of bits received from the network layer into manageable data units called as frames.

- The following are the some of the important design issues of the data link layer:
 - Services provided to the Network Layer:** The data link layer acts as a service interface to the network layer. How to provide a well-defined service interface in the network layer on source machine to the network layer on destination machine.
 - Frame Synchronization/Framing:** Frame synchronization is the major issue of data link layer. The source machine sends data in blocks called frames to be the destination machine. The starting and ending of each frame should be identified so that the frame can be recognized by the destination machine. This design issue determines how the bits of the physical layer are grouped into frames.
 - Flow Control:** It deals with how to regulate the flow of frames so that slow receivers are not swamped by fast senders.
 - Error Control:** This design issue deals with transmission errors. It must provide an error control mechanism to detect and retransmit damaged, duplicate, or lost frames from source to destination.

2.2.2 Services

- Data link layer provides several services to the network layer. The one of the major services provided is transferring the data from the network layer on the source machine to the network layer on the destination machine.
- The source machine data link layer receives the data from the network layer and the destination machine passes on this data to the network layer as shown in Fig. 2.7.

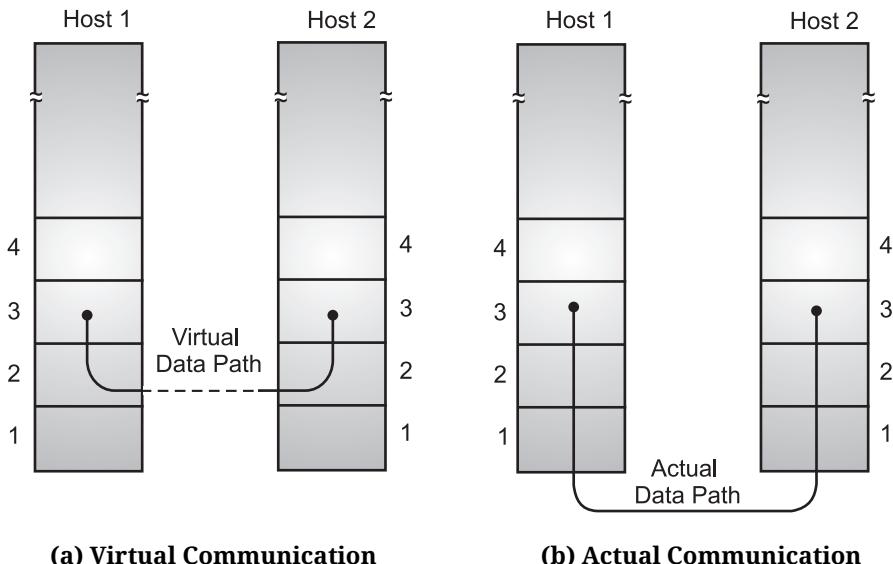


Fig. 2.7

- The path shown in Fig. 2.7 (a) is the virtual path. But the actual path is Network layer -> Data link layer -> Physical layer on source machine, then to physical media and thereafter physical layer -> Data link layer -> Network layer on destination machine.
- 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.

1. Unacknowledged Connectionless Service:

- In this service, the sender machine sends the frames to the destination machine without having the destination machine acknowledge them.
- No logical connection is established between sender and receiver beforehand. If the frame is lost, no attempt is made to detect the loss or recover from it in the data link layer.
- This is best suited when the error rate is very low, so the error recovery is left to higher layers. It is best suited for real-time traffic, in which late data is worse than bad data.
- Most LAN uses unacknowledged connectionless service.

2. Acknowledged Connectionless Service:

- In this service, no logical connection is used, but each frame sent is individually acknowledged.
- Sender knows each frame has reached safety or not. In case of any error, it can be sent again.
- This is used for unreliable channels, such as wireless systems.

3. Acknowledged Connection Oriented Service:

- Here, source and destination machines establish a connection before any data is transferred. Each frame sent in a numbered and data link layer guarantees that each frame sent is received.
- It also guarantees that each frame is received exactly once and that all frames are received in the right order. Connection oriented service provides a reliable bit stream.
- Connection-oriented has three distinct phases:
 - (i) The connection is established when some initialization takes place.
 - (ii) The actual transmission of one and more frames.
 - (iii) The connection is released freeing the variables, buffers and other resources.

2.2.3 Framing

(April 17, 18; Oct. 18)

- Framing is an important function of the data link layer. Group of physical layer bits stream into units (messages) called frames. Breaking the bit stream into frames is called framing.

- Data link layer is intermediate between the network layer and the physical layer. So the data link layer must use the services provided by the physical layer.
- Physical layer accepts raw bit stream which is not guaranteed to be error free, and attempts it to deliver it to destination.
- So it is the responsibility of the data link layer to detect errors such as the number of bits received may be less or contain different values etc.
- The data link layer breaks the bit stream into the frames and computes 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.
- One method to achieve this framing is to insert time gaps between frames. But this method is not useful because networks rarely make any guarantees about timings, so these gaps might be squeezed or other gaps might be inserted during transmission. So other methods have been devised.
- A frame is "the unit of transmission in a link layer protocol, and consists of a link layer header followed by a packet.
- Framing in the data link layer separates a message from one source to a destination by adding a sender address and a destination address.
- The destination address defines where the packet is to go; the sender address helps the recipient acknowledge the receipt.

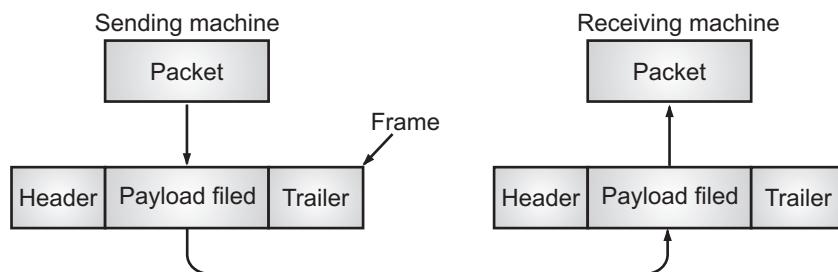


Fig. 2.8

- At the data link layer, it extracts messages from sender and provides it to receiver by providing sender's and receiver's address.
- The advantage of using frames is that data is broken up into recoverable chunks that can easily be checked for corruption.

Parts of a Frame:

- A frame has the following parts, (See Fig. 2.9):
 - 1. Frame Header:** It contains the source and the destination addresses of the frame.
 - 2. Payload Field:** It contains the message to be delivered.

3. **Trailer:** It contains the error detection and error correction bits.
4. **Flag:** It marks the beginning and end of the frame.



Fig. 2.9: Parts of Frame

2.2.4 Flow Control

(Oct. 18)

- Consider a situation, the sender is running on a fast computer (or lightly loaded) and the receiver is running on a slow (or heavily loaded) computer.
- The sender keeps on sending the frames at high speed, but the receiver is not able to accept it.
- After some time, the receiver is totally swamped out. Even though the transmission line is error free, at a certain point the receiver will be unable to handle frames and start losing them.
- To prevent such types of situations flow control mechanisms are used by the data link layers.
- Flow control is a technique for ensuring that a transmitting entity does not flood the receiving entity with data.
- The data link layer regulates flow control so that a fast sender does not drown a slow receiver.
- Flow control refers to a set of procedures used to restrict the amount of data the sender can send before waiting for acknowledgment.
- The two flow control mechanisms are Feedback-based flow control, and Rate-based flow control.
 1. In **feedback-based flow control**, the receiver sends back information to the sender giving it permission to send more data or at least telling the sender how the receiver is doing.
 2. In **rate-based flow control**, the protocol has a built-in mechanism that limits the rate at which senders may transmit data, without using feedback from the receiver.

2.2.5 Error Control

- Once the start and end of a frame is detected, the next problem is how to make sure that all frames sent by the sender are delivered to the network layer of the destination and in the proper order without error.
- Error control refers to a set of procedures that ensure that all the frames have eventually been received at the destination.

- If any frames are lost or damaged during transmission, the error control mechanism allows the receiver to inform the sender about it and coordinates the re-transmission of those frames by the sender.
- The data link layer ensures error free link for data transmission. The issues it caters to with respect to error control are:
 1. Dealing with transmission errors.
 2. Sending acknowledgement frames in reliable connections.
 3. Retransmitting lost frames.
 4. Identifying duplicate frames and deleting them.
 5. Setting timer as soon as the frame is sent (if the acknowledgment does not receive in the specified time, the same frame is retransmitted).
- If the acknowledgment does not reach before the timer runs out there will be duplicate copies of frames at the receiver end.
- To prevent this, generally a sequence number is assigned to outgoing frames. So the receiver can distinguish the retransmission.

2.2.6 Congestion Control

- A congestion is a state occurring in a network layer when the message traffic is so heavy that it slows down network response time.
- Although a link may be congested with frames, which may result in frame loss, most data-link-layer protocols do not directly use a congestion control to alleviate congestion, although some wide-area networks do.
- In general, congestion control is considered an issue in the network layer or the transport layer because of its end-to-end nature.

2.2.7 Link Layer Addressing

- The other issue about the data link layer is the link-layer addresses. An IP address is used as the identifiers at the network layer that define the exact points in the Internet where the source and destination hosts are connected.
- However, in a connectionless internetwork such as the Internet we cannot make a datagram reach its destination using only IP addresses.
- The reason is that each datagram in the Internet, from the same source host to the same destination host, may take a different path.
- The source and destination IP addresses define the two ends but cannot define which links the datagram should pass through.
- We need to remember that the IP addresses in a datagram should not be changed. If the destination IP address in a datagram changes, the packet never reaches its destination.

- If the source IP address in a datagram changes, the destination host or a router can never communicate with the source if a response needs to be sent back or an error needs to be reported back to the source.
- The above discussion shows that we need another addressing mechanism in a connectionless internet the link layer addresses of the two nodes.
- A link layer address is sometimes called link address, sometimes a physical layer, and sometimes a MAC address.
- Since, a link is controlled at the data link layer, the addresses need to belong to the data link layer.
- When a datagram passes from the network layer to the data link layer, the datagram will be encapsulated in a frame and two data link addresses are added to the frame header.
- These two addresses are changed every time the frame moves from one link to another link.

2.3 FRAMING METHODS

(April 16, 18; Oct. 18)

- The framing methods are Character count, Flag bytes with byte stuffing, Starting and ending flags, with bit stuffing and Physical layer coding violations.

2.3.1 Character Count

- Character count method uses a field in the header to specify the number of characters in the frame.
- The data link layer at destination checks the character count, it knows how many characters follow and where the end of frame is.
- Fig. 2.10 shows four frames of sizes 5, 5, 8 and 8 characters respectively.

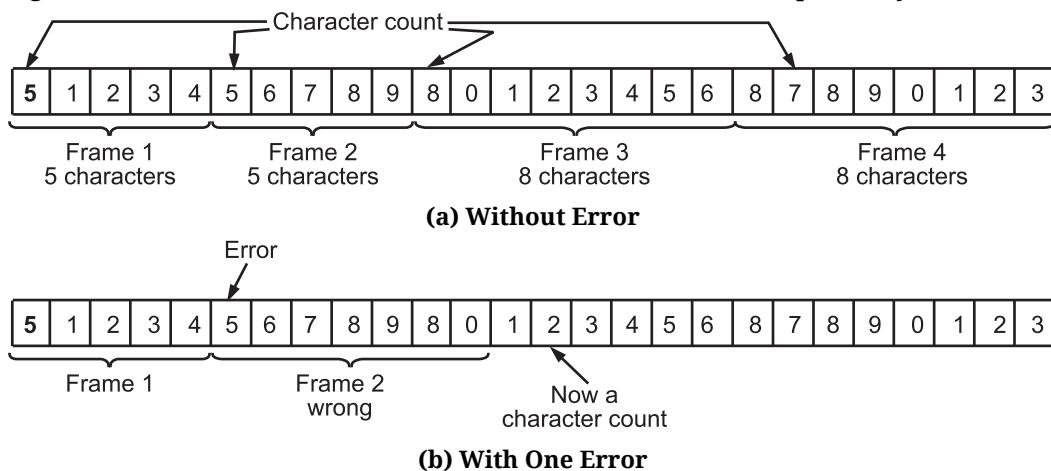


Fig. 2.10: A Character Stream

- The problem with this method is the count can be garbled by a transmission error. In Fig. 2.10 (b), the character 5 in frame 2 becomes 7, so destination frames get out of synchronization and are unable to locate the start of the next frame. So in case of any error the entire data has to be retransmitted.

2.3.2 Flag Bytes with Byte Stuffing

- The second framing method is flag byte. It solves the problem of resynchronization.
- Every frame starts and ends with a special bit pattern called a flag byte [01111110]. The flag byte is used as starting and ending delimiter as shown in Fig. 2.11.

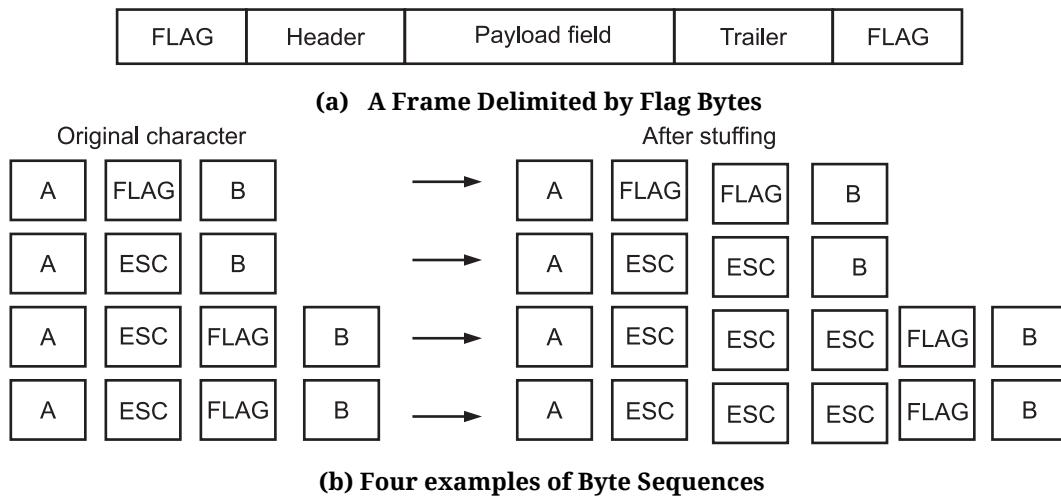


Fig. 2.11

- 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 and next frame.
- A problem here comes with the binary data or float point numbers are being transmitted. 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 removes 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.

2.3.3 Starting and Ending Flags with Bit Stuffing

(April 16)

- Here, 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 a bit stuffing.
- When the receiver sees 5 consecutive 1-bit followed by a 0-bit, it automatically de-stuffs the 0-bit. If the user data contain the flag pattern, 01111110, this is transmitted as 01111101 but stored in the receiver's memory as 01111110.
- The Fig. 2.12 shows the bit of stuffing.

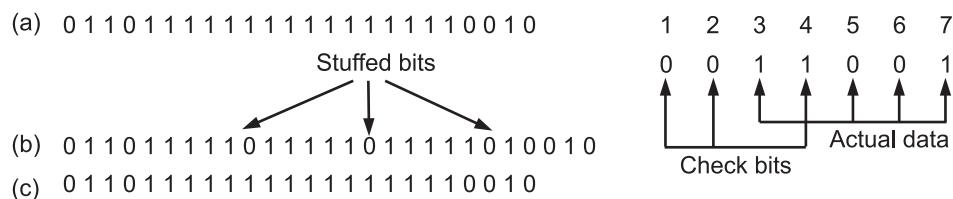


Fig. 2.12: (a) Original Data (b) The Data appear on the Line
 (c) The Data at Receivers Site

2.3.4 Physical Layer Coding Violations

- This is mainly used for the network in which the encoding contains some redundancy. Some LANs encode 1-bit by using 2 physical bits.
- A 1-bit is a high-low pair and a 0-bit is a low-high pair. Every bit has a transition in the middle. So it is easier for the receiver to locate the bit boundaries.
- Many Data link layer protocols use a combination of a character count with one of the other methods for safety.
- When the frame arrives the count field shows end of the frame. If frame delimiter is present at that position and checksum is correct the frame is accepted as valid, otherwise the input stream is scanned for the next delimiter.

2.4 CHANNEL ALLOCATION METHODS

- Data link layer is divided into two sub layers i.e., Logical Link Control (LLC) and Medium Access Control (MAC) Layer.
- The LLC provides addressing and control of the data link. MAC may refer to the sublayer that determines who is allowed to access the media at any one time.
- A 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.
- Channel allocation is a process in which a single channel is divided and allotted to multiple users in order to carry user specific tasks.
- The channel allocation problem shows how to allocate a single broadcast channel among several competing users.

- The channel might be a portion of the wireless spectrum in a geographic region, or a single wire or optical fiber to which multiple nodes are connected.
- Channel Allocation may be done using two ways Static Channel Allocation and Dynamic Channel Allocation.

2.4.1 Static Channel Allocation

- In static channel allocation, a fixed portion of the frequency channel is allotted to each competing user. This scheme is also referred to fixed channel allocation or fixed channel assignment.
- The traditional way of allocation the single channel for multiple users is the Frequency Division Multiplexing (FDM).
- If there are N users, the bandwidth is divided into N equal-sized portions, with each user being assigned one portion. Since each user has a private frequency band, there is no interference among users.
- When there is only a small and fixed number of users then FDM is a simple and efficient allocation mechanism.
- However, when the number of senders is large and continuously varying then the FDM is not suitable in those situations.
- If the total bandwidth is divided into N regions for N users and if fewer than N users are communicating, then a large piece of valuable bandwidth is wasted.
- If more than N users want to communicate, some of them will not get the permission for lack of bandwidth.

2.4.2 Dynamic Channel Allocation

- In dynamic channel allocation, frequency bands are not permanently assigned to the users. Instead channels are allotted to users dynamically as needed, from a central pool.
- Instead of reserving a special frequency band for every user and limiting the number of users, the channel is allocated dynamically which can be used to transmit the data for any number of users and at any time.
- For dynamic channel allocation, we will make some assumptions:
 1. **Station Modem:** This modem consists of N independent stations, each with a user that generates the frame of transmission. Once the frame has been generated, the station is blocked and does nothing until the frame has successfully transmitted.
 2. **Single Channel Assumption:** A single channel is available for all communication i.e. All stations can transmit or receive from it.

- 3. **Collision Assumption:** If two frames are transmitted simultaneously, they may overlap and result in the garbled signal. This event is called a collision. All stations can detect collision and the collided frames are retransmitted.
- 4. **Continuous Time:** The frame transmission can begin at any instant and there is no master clock dividing the time into discrete intervals.
- 5. **Slotted Time:** The time is divided into discrete intervals, slots. The frame transmission always begins at the start of the time slot. One-time slot may have contained transmission of many frames.
- 6. **Carriers Sense Assumption:** The station can tell if the channel is in use before trying to use it. If the channel is sensed as busy, then no station will attempt to use it until it becomes idle.
- 7. **No Carriers Sense:** Stations cannot sense the channel before trying to use it. Instead it just transmits and after some time determines whether or not the transmission was successful.
- The dynamic channel allocation is done considering a number of parameters so that transmission interference is minimized.

2.4.3 Media Access Methods

- Media access methods are implemented at the data-link layer. When nodes are connected and use a common link known as multipoint link or broadcast link, we need a multiple access protocol to coordinate access to the link.
- A channel access method or multiple access method allows more than two terminals connected to the same transmission medium to transmit over it and to share its capacity.
- Number of protocols have been divided to handle access to a shared link and categories into three groups as shown in Fig. 2.13.

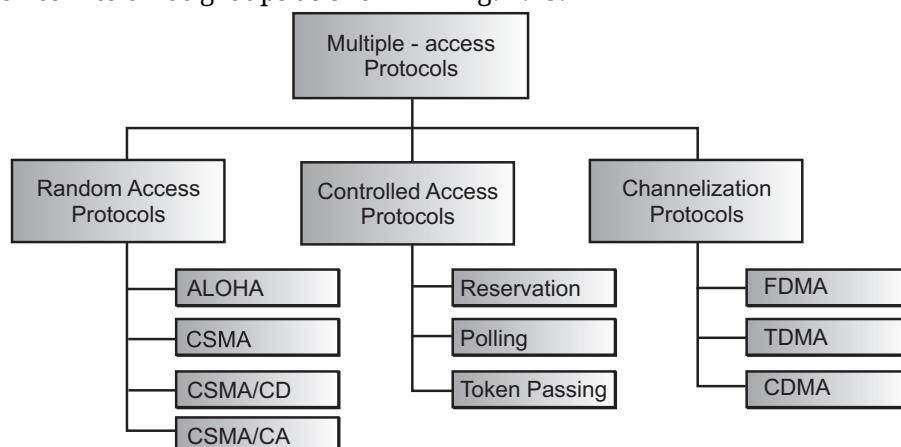


Fig. 2.13: Taxonomy of Multiple Access Protocols

- Protocols belonging to each group are shown in the Fig. 2.13.

 1. **Random Access Protocols:** In these types 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.

2.4.3.1 Random Access Protocols

(April 17, 18, Oct. 17)

- In random access or contention methods, each station in the network has equal rights.
- In random access no station is superior to other stations and none 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, a station which wants to transmit data uses a procedure defined by protocol, and decides whether to transmit or not.
- This decision depends upon whether the medium is free or busy. Random access protocols have following 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 are also called contention methods.
- 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 can a station access the medium?
 2. If the medium is busy, what station can do it?
 3. If a collision occurs, what station can do it?
 4. How does a station get information about the success and failure of a transmission?
- To answer these types of questions, we have evolved of random access methods. These are shown in Fig. 2.14.
- 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 of 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 a collision is detected.

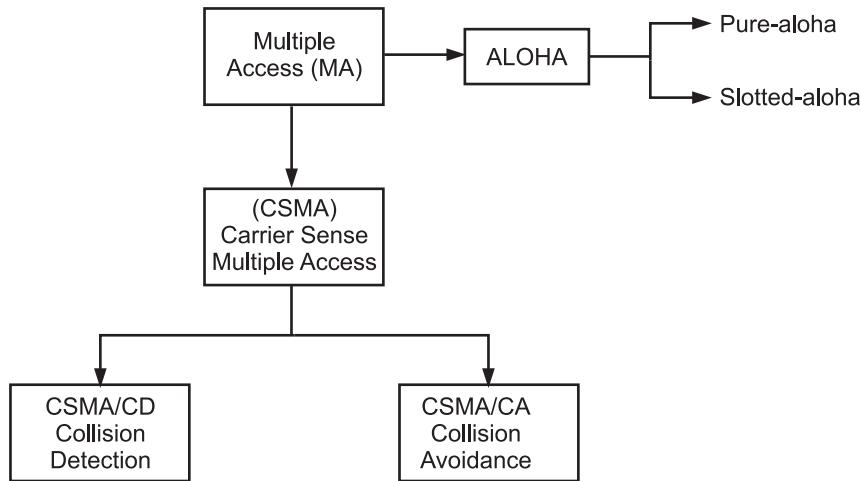


Fig. 2.14: Evolution of Random Access Methods

1. ALOHA:

(April 16, Oct. 17)

- 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 at the same time. It is obvious that the data from the two stations collide and are destroyed.
- There are two types of ALOHA protocols i.e. Pure ALOHA and Slotted ALOHA.

Pure ALOHA:

(April 16, Oct. 17)

- The original ALOHA protocol is called pure ALOHA. Concept of ALOHA is very simple; each station sends a frame whenever it has a frame to send.
- Since there is only one channel to share, there is possibility of collisions between frames from different stations.
- Fig. 2.15 shows an example of frame collisions in pure ALOHA.
- In Fig. 2.15 as an example four stations are shown. Every station sends frames on a 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.

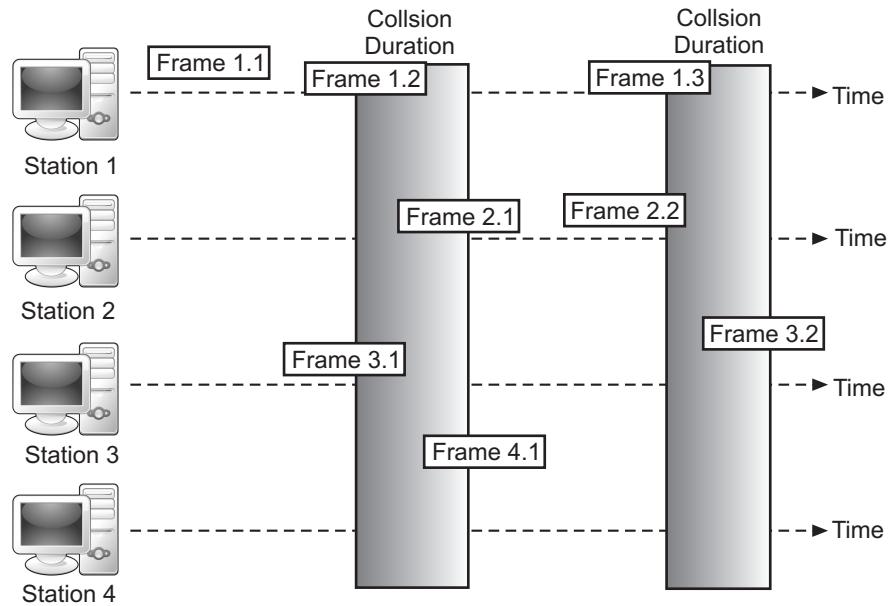


Fig. 2.15: Frames in Pure ALOHA

- 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 a collision the station waits for a random amount of time and sends it again. This waiting time must be random otherwise the same frames will collide again and again.
- Therefore, pure ALOHA dictates that when the 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.
- The pure ALOHA protocol has a second method to prevent congesting the channel with retransmissions. It is shown in Fig. 2.16.
- 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 the station has to use a back-off strategy and send the packet again. After several tries, if it is not happening then procedure is aborted.
- Vulnerable Time:** Vulnerable time is a time in which there is possibility of collision. It is calculated as,

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

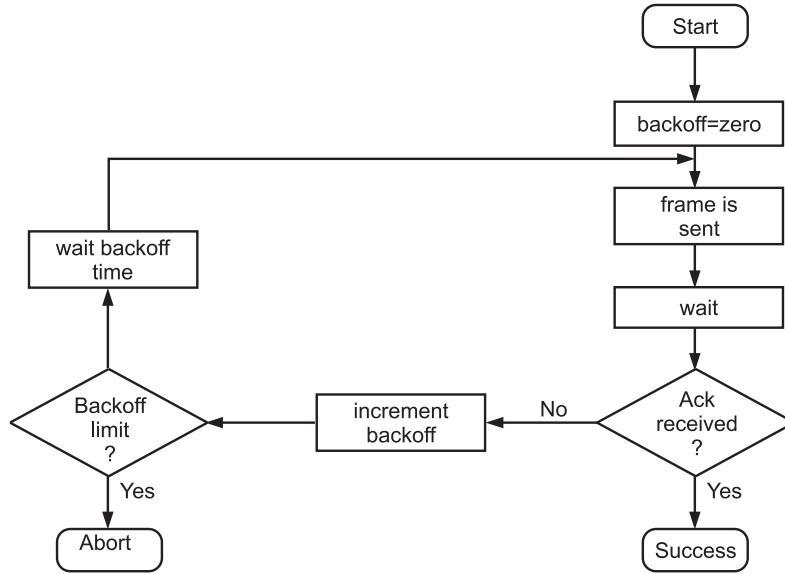


Fig. 2.16: ALOHA Protocol Procedure

- **Throughput:** Let G be the average number of frames generated by the system during one frame transmission time. Then the average number of successful transmissions 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 %.

Slotted ALOHA:

(April 16; Oct. 17)

- An improvement to the original ALOHA protocol was "Slotted ALOHA", which introduced discrete time slots 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. 2.17.
- Slotted ALOHA still has an edge over pure ALOHA as chances of collision are reduced to one-half. Slotted ALOHA requires global time synchronization.

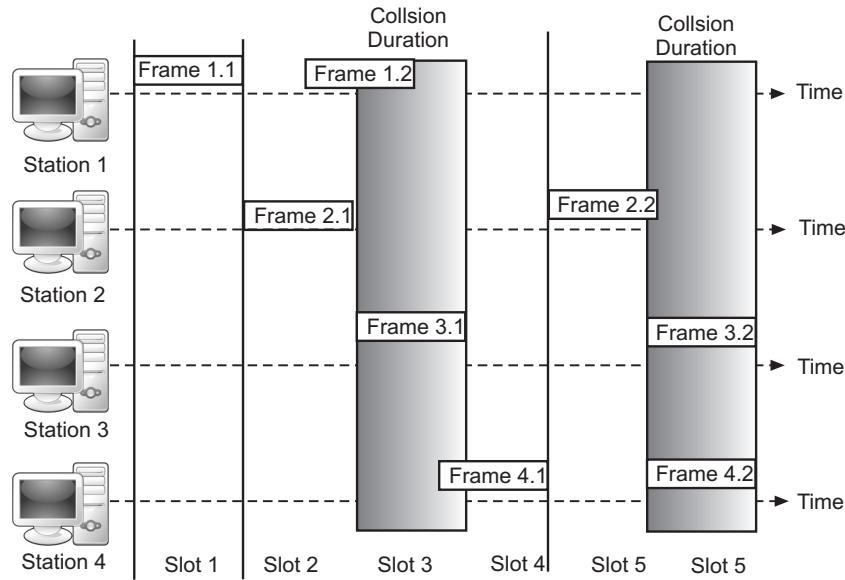


Fig. 2.17: Frames in Slotted ALOHA

2. Carrier Sense Multiple Access (CSMA):

(April 17, 18; Oct. 17)

- To minimize the chance of collision and increase the performance, the CSMA method was developed. The chance of a collision can be reduced if a station senses the medium before trying to use it.
- Protocols in which stations listen for a carrier and act accordingly are called Carrier Sense Protocols.
- 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.
- 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. 2.18.

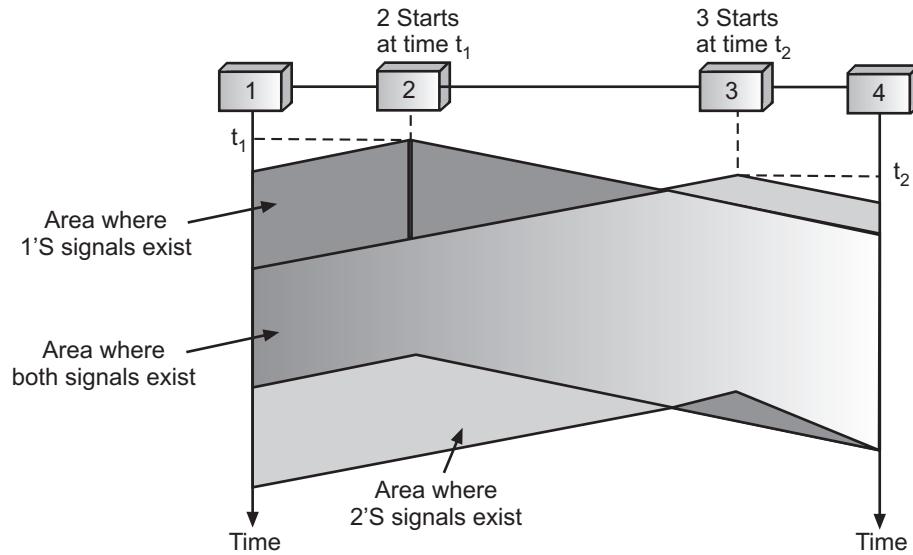


Fig. 2.18: Time/Space Model of the Collision in CSMA

Vulnerable Time:

- The vulnerable time for CSMA is the propagation time T_{p_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 themselves from sending.

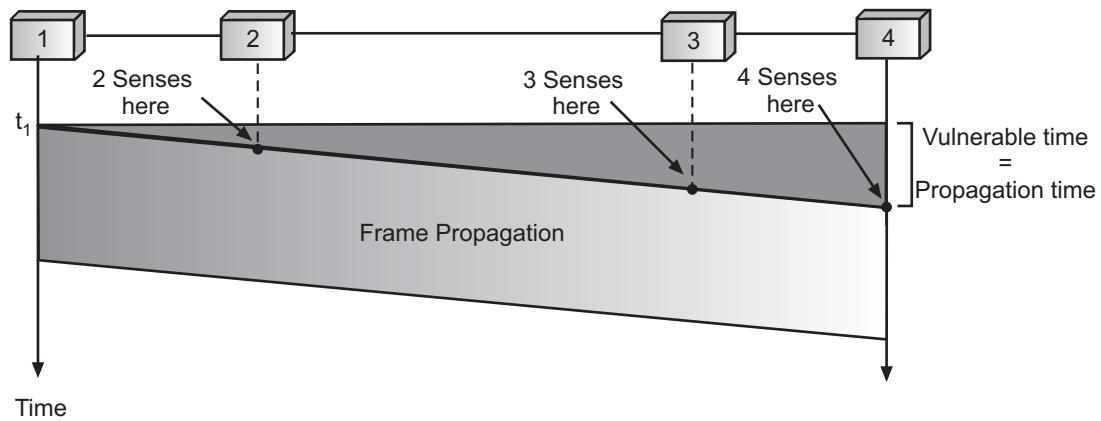


Fig. 2.19: Vulnerable Time for CSMA

Persistence Methods:

- If the channel is free definitely stations will transmit data. But if the channel is busy, what should a station do? Three different protocols are invented for this.

- There are three different types of CSMA protocols i.e., I-persistent CSMA, Non-persistent CSMA and P-persistent CSMA as shown in Fig. 2.20.

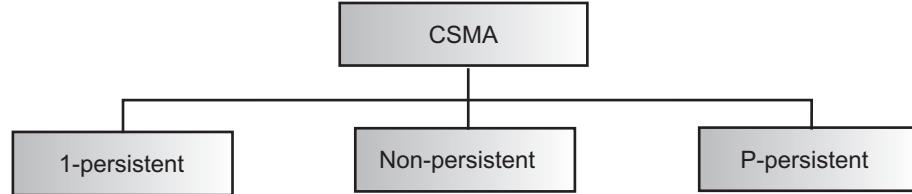


Fig. 2.20: Types of CSMA

1-persistent CSMA:

- This method is very simple and straightforward. In 1-persistent CSMA method, a 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 I-persistent CSMA.
- This method has the highest chance of collision because two or more stations may find the channels 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.

Drawback of 1-persistent CSMA:

- The propagation delay time greatly affects this protocol. Let us suppose, just after the station I begins its transmission, station 2 also becomes ready to send its data and senses the channel.
- If the station I 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 a collision.

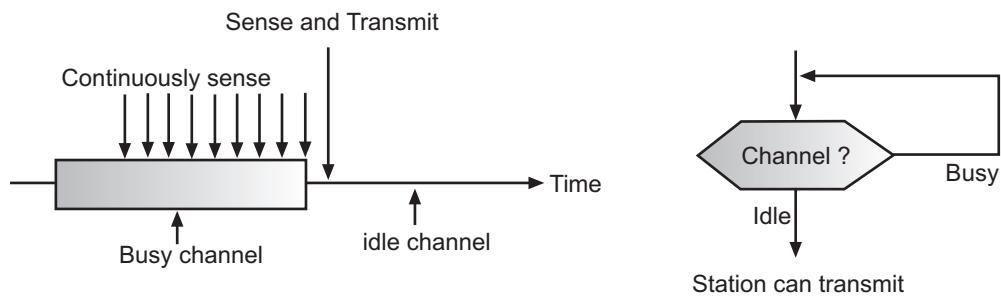


Fig. 2.21: 1-persistent CSMA

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

Non-persistent CSMA:

- In non-persistent CSMA, a station that has a frame to send senses to 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.
- 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.

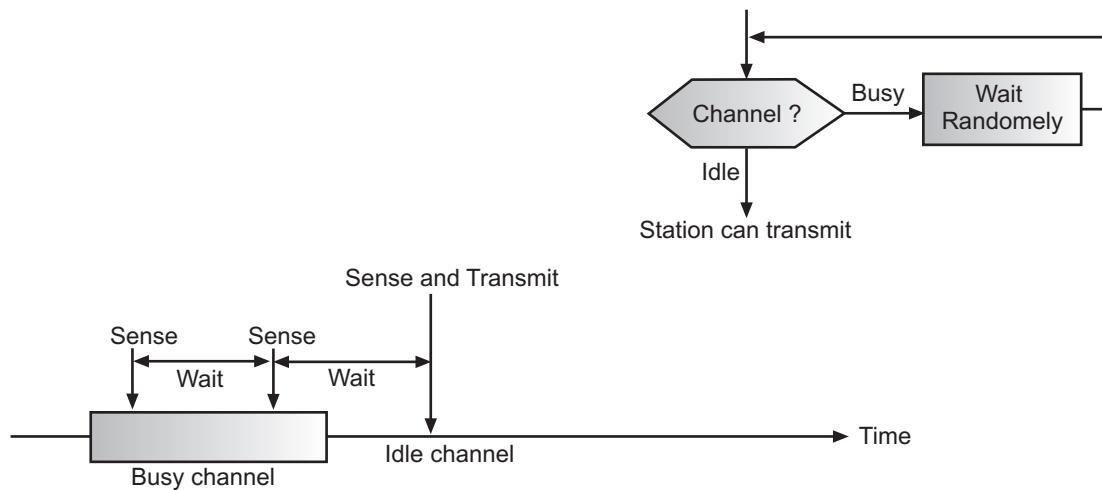


Fig. 2.22: Non-persistent CSMA

Advantage of Non-persistent CSMA:

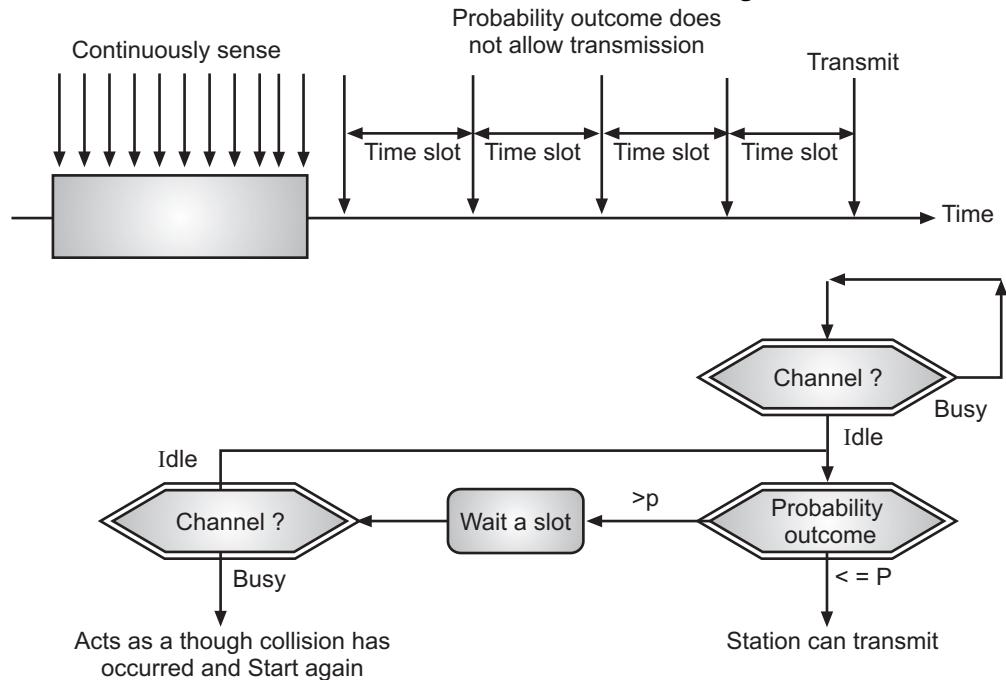
- It reduces the chance of collision because the stations wait a random amount of time.
- It is unlikely that two or more stations will wait for the same amount of time and will retransmit at the same time.

Disadvantage of Non-persistent CSMA:

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

P-persistent CSMA:

- This method is used when a 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 the channel is busy, the station waits until the next slot.
- If the 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.
- 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 though a collision has occurred and it waits a random amount of time and starts again.

**Fig. 2.23: P-persistent CSMA**

- Advantage of p-persistent CSMA is it reduces the chance of collision and improves the efficiency of the network.

3. CSMA/CD:

(April 16; Oct. 17)

- CSMA/CD stands for Carrier Sense Multiple Access with Collision Detection. CSMA/CD is a protocol in which the station senses the carrier or channel before transmitting frames just as in persistent and non-persistent CSMA.

- If the channel is busy, the station waits. The wastage of channel time problem is handled in CSMA/CD.
- In CSMA/CD, the station that places its data onto the channel after sensing the channel continues to sense the channel even after the data transmission.
- If a collision is detected, the station aborts its transmission and waits for a predetermined amount of time and then sends its data again. As soon as a collision is detected, the transmitting station releases a jam signal.
- Jam signals will alert the other stations. The stations are not supposed to transmit immediately after the collision has occurred. Otherwise there is a possibility that the same frames would collide again.
- After some back-off delay time the stations will retry the transmission. If the collision occurs again then the back off delay time is increased progressively.
- Therefore, the CSMA/CD method consists of alternating transmission periods and collisions with idle periods when none of the stations is transmitting.

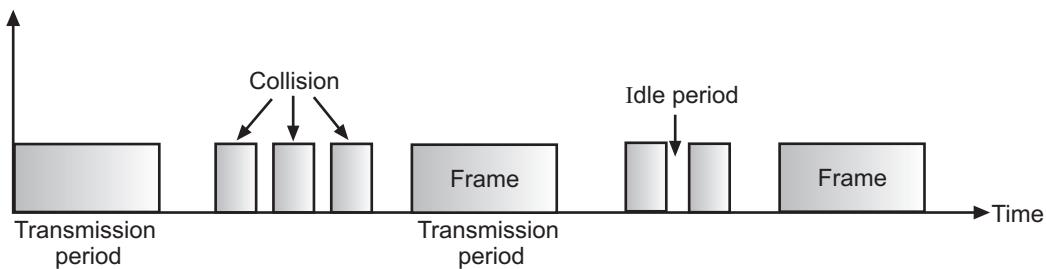


Fig. 2.24: CSMA/CD with Three States

- The entire scheme of CSMA/CD is depicted in Figs. 2.25 and 2.26.

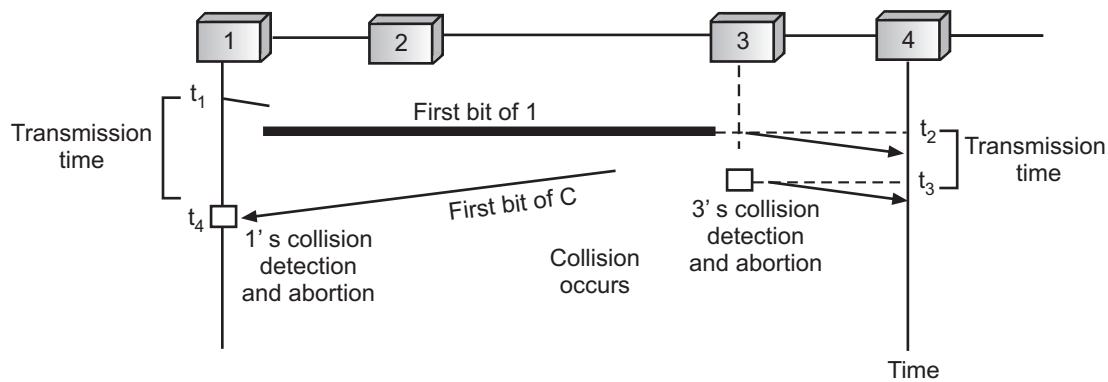


Fig. 2.25: Collision of the First Bit in CSMA/CD

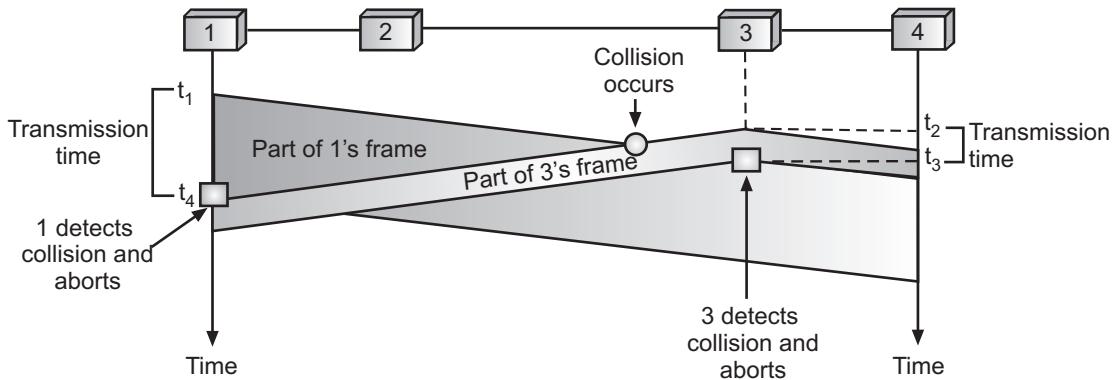


Fig. 2.26: Collision and Abortion in CSMA/CD

CSMA/CD Procedure:

- Fig. 2.27 shows a flow chart for the CSMA/CD protocol.

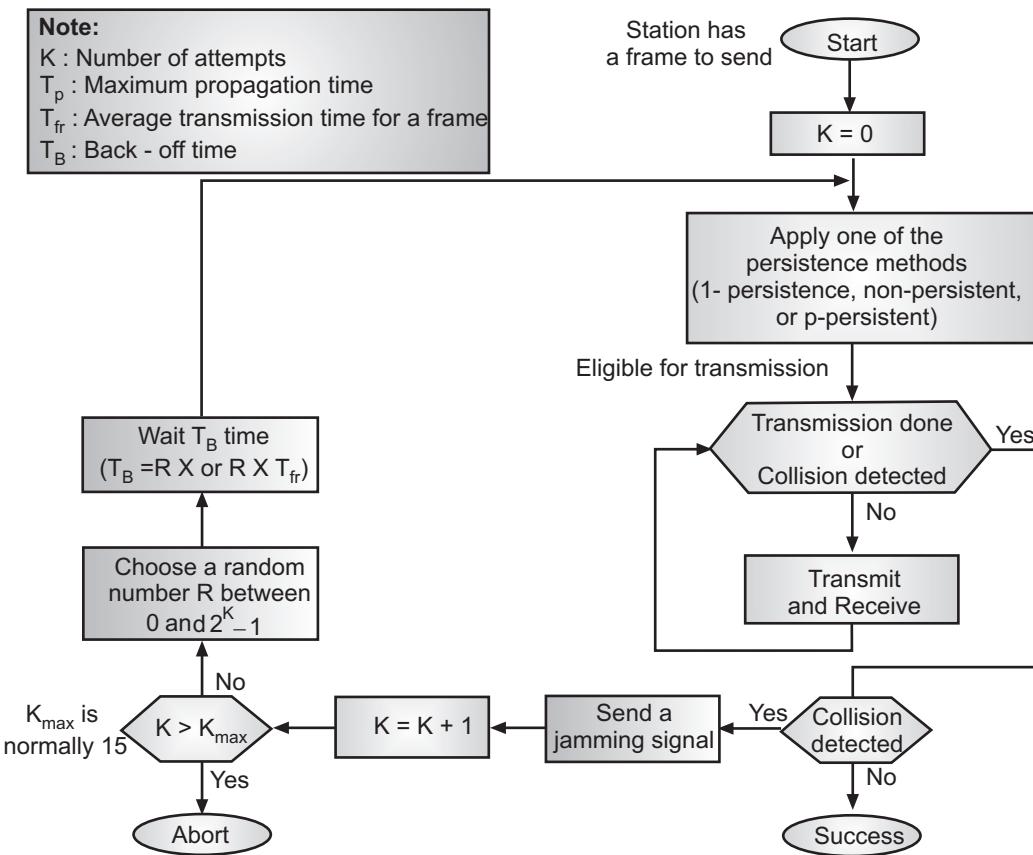


Fig. 2.27: Flowchart for the CSMA/CD Protocol

Explanation of Fig. 2.27:

- 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.
- If so, send 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 CSMA/CD. 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.

4. CSMA/CA:**(Oct. 17, April 18)**

- 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, the station receives its own signal. When there is a 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 collisions.
- It is particularly important for wireless networks, where the collision detection of the alternative CSMA/CD is unreliable due to the hidden node problem.
- So to avoid collision in wireless networks, because they cannot be detected we need another protocol. 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. 2.28.
 - (i) Inter frame space,
 - (ii) Contention window, and
 - (iii) Acknowledgements.

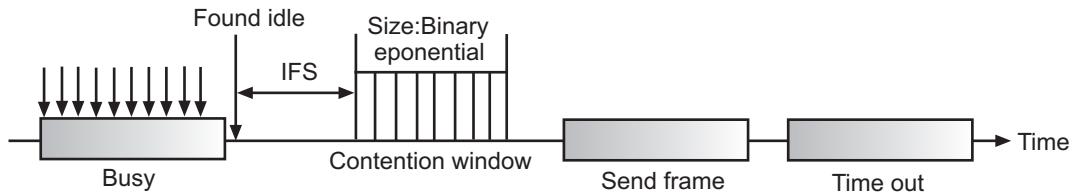


Fig. 2.28: Three Basic Techniques for Collision Avoidance

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 the channel is sensed to be idle, it may be possible that the 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 variables can also be used to define the priority of a station or a frame.

2. Contention Window:

- The 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 for 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 the 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 the receiver has received the frame.

CSMA/CA Procedure:

- Fig. 2.29 shows the flow chart explaining the principle of CSMA/CA.

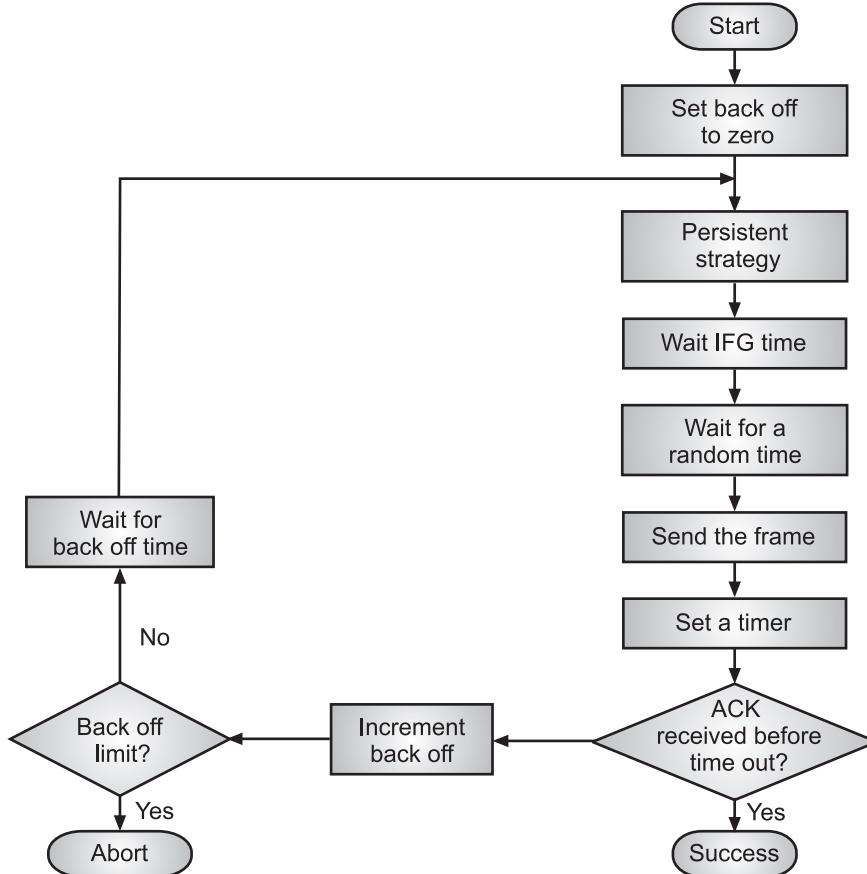


Fig. 2.29: CSMA/CA Procedure

Explanation of Fig. 2.29:

- 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 so 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 expires then it increments the back off parameter, waits for the back off time and re-senses the line.

2.4.4 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 area namely, Reservation, Polling, and Token passing.

1. Reservation:

(Oct. 18; April 19)

- In this method, the station needs to make a "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 reservations to send the data frame. In each interval a reservation frame precedes the data frame.
- Fig. 2.30 shows this scenario.

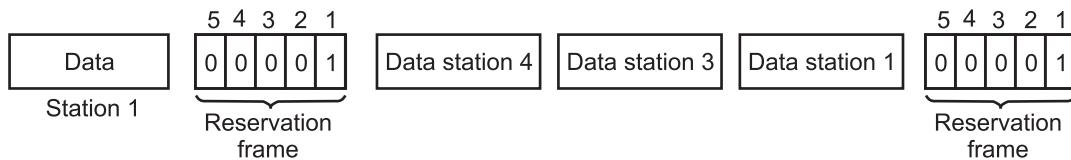


Fig. 2.30: Reservation Method in the Controlled Access

- Fig. 2.30 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.

2. Polling:

(April 16, 19)

- In this method, one station is designated as a primary station and others are secondary stations. All data transfer should be made through the primary device.
- Primary device controls the link and acts as a master. All secondary devices follow its instructions.
- The primary device decides as to which device is allowed to use the channel. If the primary station wants to receive data, it asks the secondaries if they have anything to send. This method is called polling.
- If the primary station wants to send data, it asks the secondary station to receive the data. This is called selecting.

1. Select:

(April 16, 17, 18, 19; Oct. 17, 18)

- This is used when the primary device sends the data. When the 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 sent.

2. Poll:

- Whenever primary wants to receive data then polling is used. It polls each machine, if it has something to send.
- The secondary response with MAK 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 MAK 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. 2.31 shows select and poll functions in the polling access method.

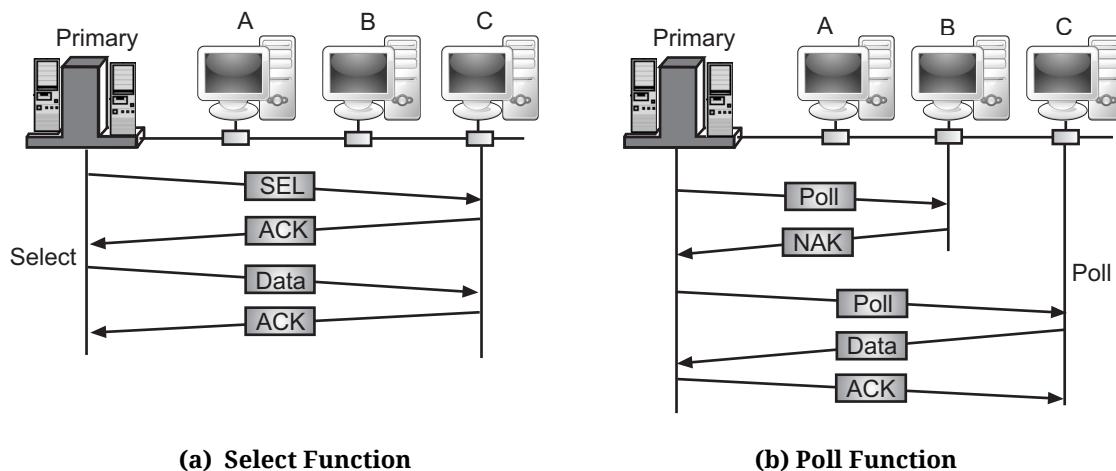


Fig. 2.31

3. Token Passing:

- In this method, a station is allowed to send data when the station receives a special frame called a token.
- In token passing, the stations are organized in a logical ring. For every station there is a predecessor and a successor.
- 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.
- Fig. 2.32 shows concepts of token passing.

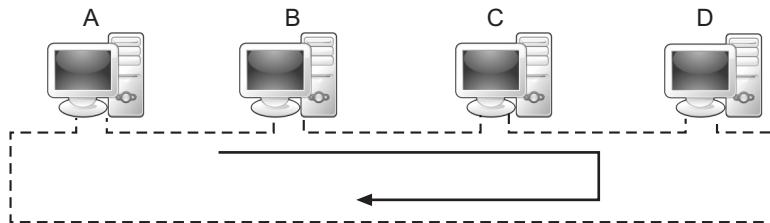


Fig. 2.32: Token Passing

- When the channel is idle then the token circulates around the ring. When the 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).
- Token management is needed for this access method. The token must be monitored to ensure it has not been lost or destroyed.
- The procedure is as shown in Fig. 2.33.

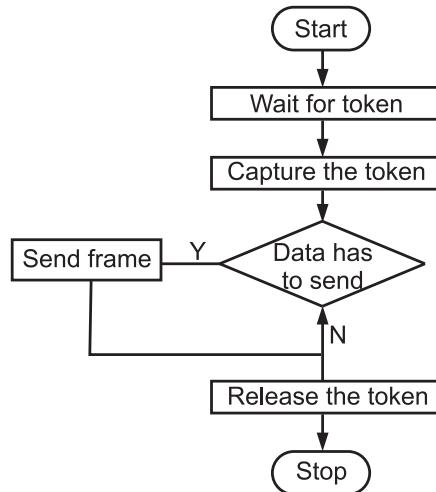


Fig. 2.33: Flowchart for Token Passing Procedure

2.4.5 Channelization

(April 16, 17, 19; Oct. 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.
- Sometimes channelization is also called as channel partition. The three channelization protocols present in networking are FDMA, TDMA and CDMA.
- In FDMA (Frequency Division Multiple Access), 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.

- In 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 sent.
- In CDMA (Code Division Multiple Access), 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.

1. FDMA:

(April 17, Oct. 18)

- 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.
- 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 interference.
- FDM is a physical layer technique whereas FDMA is an access method in the data link layer.
- 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.

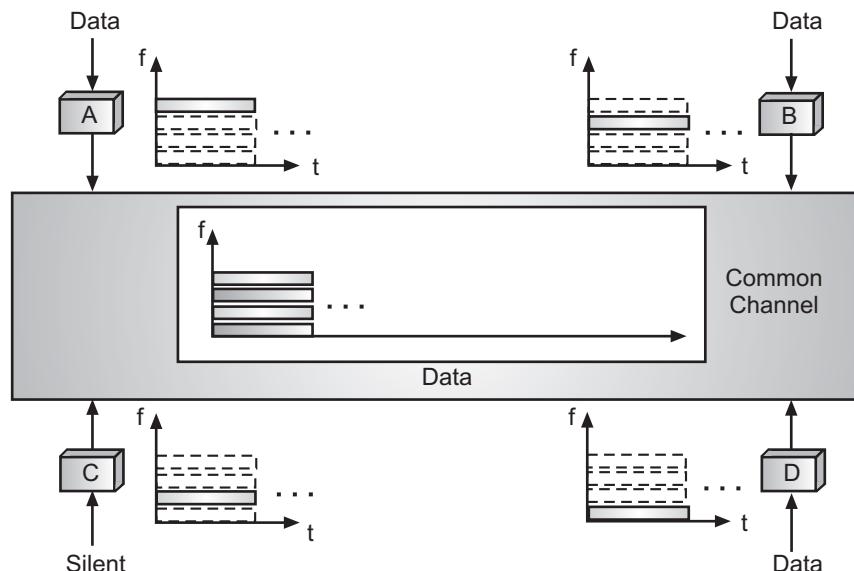


Fig. 2.34: Concept of FDMA

- 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. 2.34 shows the FDMA concept.

2. TDMA:

- TDMA is a channel access method for stored medium networks.
- TDMA stations share the bandwidth of the channel in time. Every station is allocated a time slot, in which it can send data.
- TDMA is a digital technique that divides a single channel or band into time slots.
- In TDMA every station needs to know the beginning of its slot and the location of its slot. To compensate for the delays guard spaces are used.
- In TDMA, the bandwidth is just one channel that is time shared between different stations.

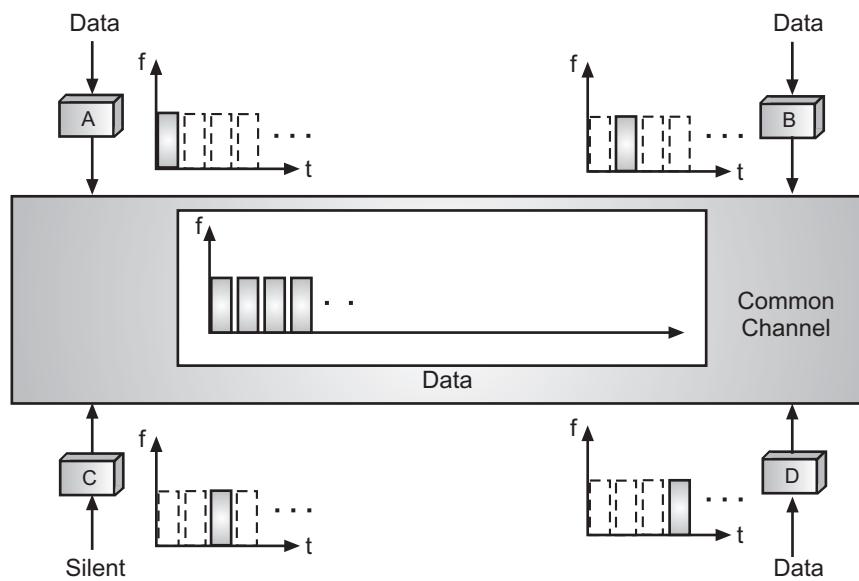


Fig. 2.35: TDMA Method

- TDMA and TDM seem to be conceptually the same, but they are different. TDM is a physical layer technique, whereas TDMA is a Data link layer access method.
- The Data link layer in each station tells its Physical layer to use the allocated time slot.

3. CDMA:

(Oct. 17)

- CDMA means communication with different codes. For example, consider a large hall with many people. Some of them understand only English, some Hindi, some Chinese etc.

- The people communicate with a language, which they understand. The common channel (hall) allows communication between several people, but in different languages (codes).
- CDMA is also called spread-spectrum and code division multiplexing, one of the competing transmission technologies for digital mobile phones.
- The transmitter mixes the packets constituting a message into the digital signal stream in an order determined by a Pseudo-Random Number (PRN) sequence.
- PRN is also known to the intended receiver, which uses it to extract those parts of the signal intended for itself. Hence, each different random sequence corresponds to a separate communication channel.
- Unlike TDMA, in CDMA all stations can transmit data simultaneously, there is no timesharing. CDMA allows each station to transmit over the entire frequency spectrum all the time.
- Multiple simultaneous transmissions are separated using coding theory. In CDMA each user is given a unique code sequence.

2.5 SWITCHING AND TCP/IP LAYERS

- Switching can happen at several layers of the TCP/IP protocol suite like Physical Layer, Data Link Layer and Application Layer.
- At the physical layer of the TCP/IP protocol suite, we can have only circuit switching.
- There are no packets exchanged at the physical layer. The switches at the physical layer allow signals to travel in one path or another.
- At the data link layer of the TCP/IP protocol suite, we can have packet switching. However, the term packet in this case means frames or cells.
- Packet switching at the data link layer of the TCP/IP protocol suite is normally done using a virtual-circuit approach.
- At the application layer of the TCP/IP protocol suite, we can have only message switching. The communication at the application layer occurs by exchanging messages.
- Conceptually, we can say that communication using e-mail is a kind of message-switched communication, but we do not see any network that actually can be called a message-switched network.

2.5.1 Types of Switching

- 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. 2.36 shows switched network.

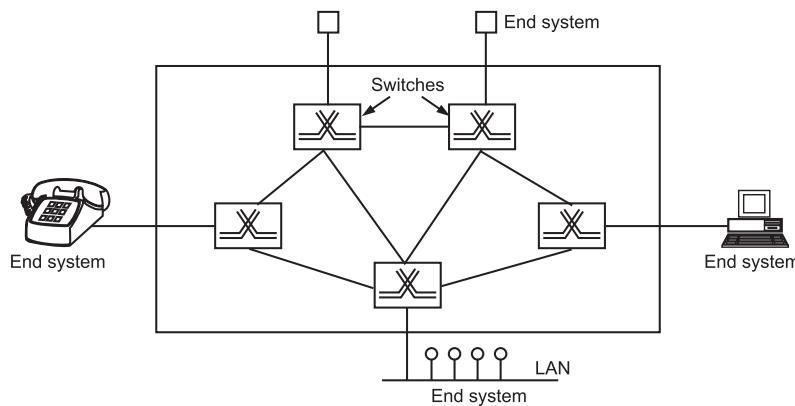


Fig. 2.36: Switched Network

- There are basically three types of switching methods available namely, Circuit Switching, Packet Switching and Message Switching as shown in Fig. 2.37.

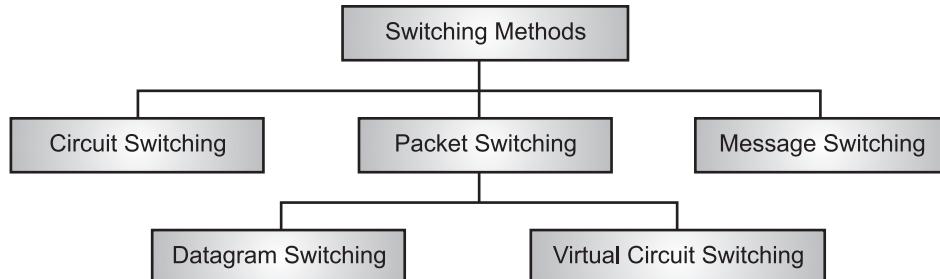


Fig. 2.37: Types of Switching

- Circuit and packet switching are commonly used today. Message switching has been phased out in general communications.

2.5.1.1 Circuit Switching

(April 16, 18)

- Circuit switching takes place at the physical layer of the TCP/IP reference model. Circuit switched networks consist of a set of switches connected by physical links.

- In a circuit switched network, two nodes communicate with each other over a dedicated communication path.
- 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. 2.38 shows the concept of circuit switching. In Fig. 2.38, 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.

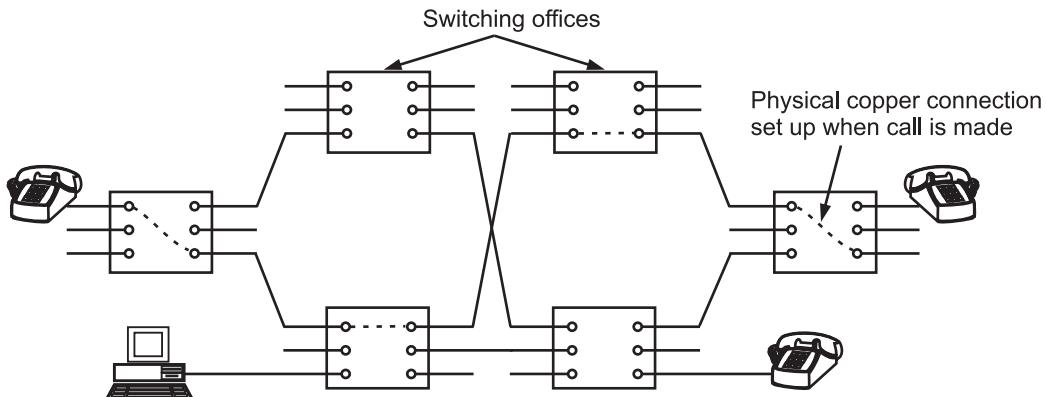


Fig. 2.38: Circuit Switching

- 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:
 - 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.
 - 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 of Circuit Switching:

1. The dedicated path/circuit established between sender and receiver provides a guaranteed data rate.
2. Once the circuit is established, data is transmitted without any delay as there is no waiting time at each switch.
3. Less expensive.
4. Fixed transit delays and throughput.
5. No loss of packets or out of order packets here as this is connection oriented network unlike packet switched network.

Disadvantages of Circuit Switching:

1. As it is designed for voice traffic, it is not suitable for data transmission.
2. Circuit switching is usually done using a fixed rate stream (for example, 64 Kbps).
3. Circuit switched networks do not provide flow control nor error control.
4. Dedicated channels require more bandwidth.
5. It is more expensive compared to other techniques due to dedicated path requirements.
6. Because connections are not shared, more links must be available to ensure new connections are not blocked.

2.5.1.2 Packet Switching

(Oct. 17)

- In packet switching, messages are divided into packets of fixed or variable size. The size of the packet is determined by the network and the governing protocol.
- Packet switching approach was developed for long-distance data communication (1970) and it has evolved over time.
- In packet switching is shown in Fig. 2.39. The data are transmitted in short packets (few Kbytes).
- In packet switching, each packet has source and destination addresses, travelling from one point (router) to the other point (router).
- Every packet contains some control information in its header, which is required for routing and other purposes.

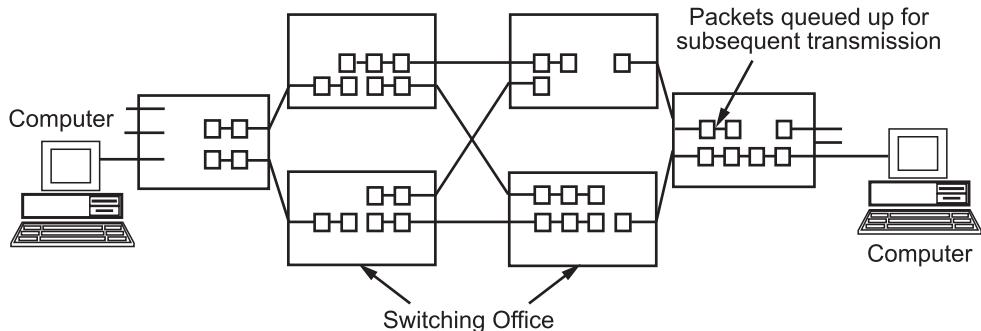


Fig. 2.39: Packet Switching

Advantages:

1. In packet switching, no circuit set up is required in advance.
2. In packet switching, the quality of data transmission is kept high (error free).
3. In packet switching, no bandwidth is reserved.
4. Packet switching is more fault tolerant.
5. Better utilization of the network segments in terms of the usage of the network path.
6. Efficient for busty data and efficient used network paths.
7. In packet switching, computers at each node allow dynamic data routing.

Disadvantages:

1. In packet switching, different packets can follow different paths, so they may arrive out of order.
2. If the network becomes overloaded, packets are delayed or discarded or dropped. This leads to retransmission of lost packets by the sender. This often leads to loss of critical information if errors are not recovered.
3. Packet switching network cannot be used in applications requiring very little delay and higher quality of service e.g., reliable voice calls.
4. Protocols used in the packet switching are complex and require high initial implementation costs.
- The two types of packet switching are Datagram Packet Switching and Virtual Circuit Packet Switching.

Datagram Packet Switching:

(Oct. 18)

- In a datagram network, each packet is routed individually by network devices based on the destination address contained within each packet.
- Due to each packet is routed individually, the result is that each packet is delivered out-of-order with different paths of transmission, it depend on the networking devices like (switches and routers) at any given time.

- After reaching the recipient location, the packets are reassembling to the original form. Datagram packet switching is normally implemented in the network layer. Each packet carries a header that contains the full information about the destination.
- When the switch receives the packet, the destination address in the header of the packet is examined; the routing table is consulted to find the corresponding port through which the packet should be forwarded.

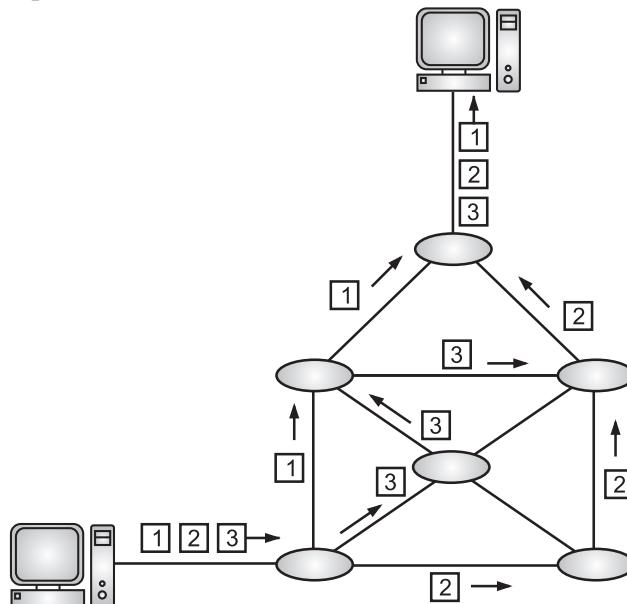


Fig. 2.40: Datagram Packet Switching

Advantages of Datagram Packet Switching:

1. No call setup phase required.
2. More flexible because routing can be used to avoid congested ports of the network.
3. Cheaper in cost.

Disadvantages Datagram Packet Switching:

1. Packets are forwarded slowly as compared to the virtual circuit approach.
2. Processing time requests more at node.

Virtual Circuit Packet Switching:

(Oct. 18)

- In this type of network switching, packets are sent in sequential order over a defined route. Virtual circuit packet switching is normally done at the data link layer.
- Virtual circuit packet switching establishes a fixed path between a source and a destination to transfer the packets.
- A source and destination have to go through three phases in a virtual circuit packet switching:
 1. Setup phase.

- 2. Data transfer phase.
- 3. Connection release phase.
- A logical connection is established when a sender sends a setup request to the receiver and the receiver sends back an acknowledgement to the sender if the receiver agrees.
- All packets belonging to the same source and destination travel the same path. The information is delivered to the receiver in the same order as transmitted by the sender.

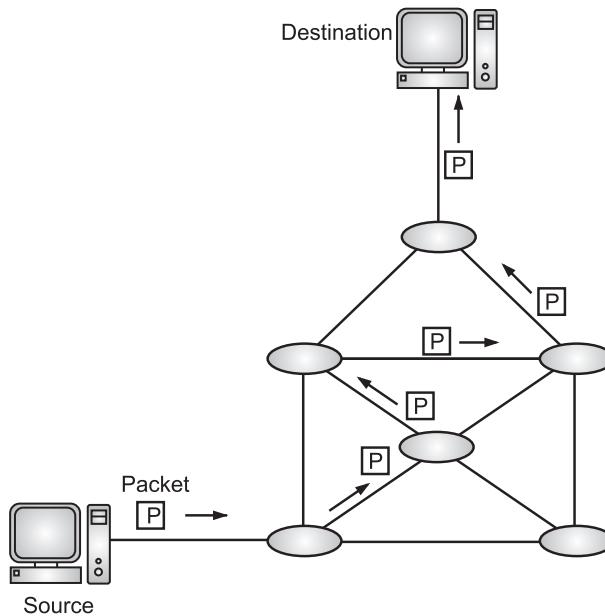


Fig. 2.41: Virtual Circuit Packet Switching

Advantages of Virtual Packet Circuit Switching:

1. Virtual circuit provides packet sequencing and error control.
2. Packet forwarding is fast and quick.
3. Multiple packets sent by the same source to the same destination.

Disadvantages of Virtual Packet Circuit Switching:

1. Loss of a node losses all circuits through that node so it is less reliable.
2. Less flexible than other approaches.
3. Cost is higher than the datagram approach.

Virtual Circuit Approaches:

1. **Switched Virtual Circuit (SVC):** SVC format is comparable to dial up lines in circuit switching.
2. **Permanent Virtual Circuit (PVC):** These are comparable to leased line in circuit switching.

Comparison between SVC and PVC:

Sr. No.	SVC	PVC
1.	SVC stands for Switched Virtual Circuit.	PVC stands for Permanent Virtual Circuit.
2.	In SVC a source and a destination connect when data is being transferred.	In PVC a source and a destination may choose to have a PVC.
3.	SVC creates a temporary short connection.	PVC creates a permanent and continuous connection.
4.	Cheapest in cost.	Cost is high.
5.	Examples: ATM, X.25, etc.	Examples: Frame Relay, X.25, etc.

Comparison of Datagram Approach and Virtual Circuit Packet Switching:

Sr. No.	Datagram Packet Switching	Virtual Circuit Packet Switching
1.	All packets are free to go to any path on any intermediate router which is decided on the go by dynamically changing routing tables on routers.	First packet goes and reserves resources for the subsequent packets which as a result follow the same path for the whole connection time.
2.	More flexible because routing can be used to avoid congested port of the network.	Less flexible.
3.	Slow in packet forwarding.	Packets are forwarded quickly.
4.	More reliable.	Less reliable because loss of node losses all circuits through that node.
5.	It is a connectionless service.	It is a connection-oriented service.
6.	No circuits or path established.	Virtual circuits are established between source and destination before data transfer.
7.	Out of order data delivery.	Sequential type of delivery.
8.	No resource allocation required.	Resources are allocated on demand.

Contd...

9.	Unreliable.	Virtual circuits are highly Reliable.
10.	Unpredictable delay.	High delay.
11.	Example: Internet.	Example: X.25, Frame Relay.
12.	Implementation is easy and cost efficient.	Implementation of virtual circuits is costly.

2.5.1.3 Message Switching

- In message switching, it is not necessary to establish a dedicated path between transmitter and receiver. In this, each message is routed independently through the network.
- In message switching, each message carries a header that contains the full information about the destination.
- In message switching, the message is sent to the nearest directly connected switching node as shown in Fig. 2.42.
- This node stores the message, checks for errors, selects the best available route and forwards the message to the next intermediate node.
- Each intermediate device receives the message and stores it until the next device is ready to receive it and then this message is forwarded to the next device.
- For this reason, a message switching network is sometimes called a **Store and Forward Switching**.

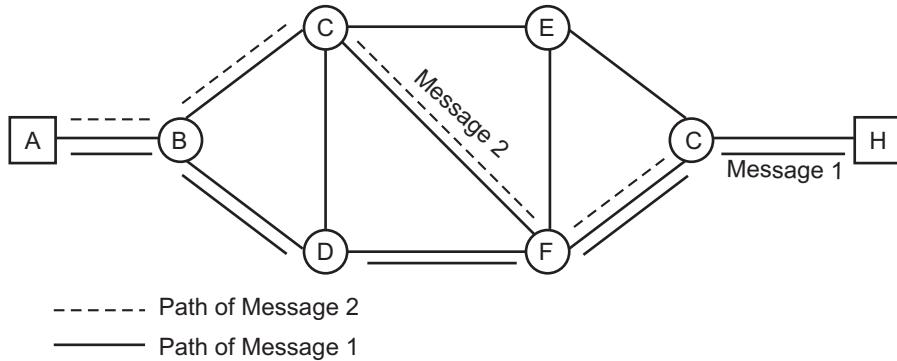


Fig. 2.42: Message Switching Technique

Advantages:

- In message switching, no circuit setup is required in advance.
- As more devices share the same channel simultaneously for message transfer, it has higher channel efficiency compared to circuit switching.
- Data rate conversion is possible in message switching.

4. Message switching, supports message lengths of unlimited size.
5. It is possible to incorporate priorities to the messages as they use store and forward technique for delivery.

Disadvantages:

1. Message switching type does not establish a dedicated path between the devices. As there is no direct link between sender and receiver, it is not reliable communication.
2. The method is costly as store and forward devices are expensive. This is due to large storage disks requirements to store long messages for long duration.
3. Message switching is not compatible for interactive applications such as voice and video. This is due to longer message delivery time.
4. Message switching is very slow because of store-and-forward technique.

Difference between Message Switching, Packet Switching and Circuit Switching:

Sr. No.	Parameters	Message Switching	Circuit Switching	Packet Switching
1.	Concept	In message switching, each switch stores the whole message and forwards it to the next switch. Although we don't see message switching at lower layers, it is still used in some applications like electronic mail (e-mail).	When the computer places a telephone call, the switching equipment within the telephone system seeks out a physical path all the way from your telephone to the receiver's telephone. This technique is called circuit switching.	With this technology, packets are sent as soon as they are available.
2.	Store and forward transmission	Yes.	No.	Yes.
3.	Addressing	Geographical addresses.	Hierarchical numbering plan.	Hierarchical address space.
4.	Routing	Manual routing.	Route selected during call setup.	Each packet routed independently.

Contd...

5.	Multiplexing	Character multiplexing, message multiplexing.	Circuit multiplexing.	Packet multiplexing shared media across networks.
6.	Call setup	No.	Required.	Not needed.
7.	Dedicated physical path	Not required.	Yes.	No.
8.	Bandwidth available	--	Fixed.	Dynamic.
9.	Application	Telegraph network for transmission of telegrams.	Telephone network for bidirectional, real time transfer of voice signals.	Internet for datagram and reliable stream service between computers.
10.	End Terminal	Telegraph, Teletype.	Telephone, modem.	Computer.
11.	Information Type	Morse, Baudot, ASCII.	Analog voice or PCM digital voice.	Binary Information.
12.	Transmission system	Digital data over different transmission media.	Analog and Digital data over different transmission media.	Digital data over differential transmission media.

2.6 WIRED LANs

- In Chapter 1, we learned that a Local Area Network (LAN) is a computer network for the home and small business is designed for a limited geographic area (less than) such as a building or campus.
- Most LANs today are also linked to a Wide Area Network (WAN) or the Internet.
- Wired networks are the most common type of Local Area Network (LAN) technology. A wired network (LAN) is simply a collection of two or more computers, printers, and other devices linked by Ethernet cables.
- LANs can be built using either wired or wireless technology. LAN supports several technologies such as Ethernet, Token Ring, Token Bus, FDDI, and ATM LAN.
- The Institute of Electrical and Electronic Engineers (IEEE) developed a series of networking standards for LANs. These standards are collectively known as IEEE 802.

- Today Ethernet is by far the dominant technology. Other technologies survived for a while. Fig. 2.43 shows an example of four computers connected in a traditional Ethernet LAN.

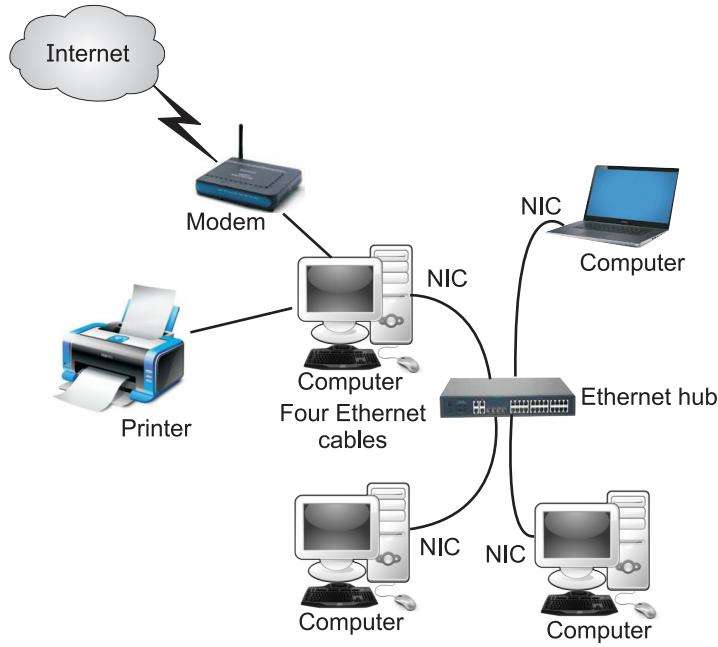


Fig. 2.43: A Traditional Ethernet LAN

- The IEEE has subdivided the data link layer into two sub layers i.e. LLC (Logical Link Control) and MAC (Media Access Control).

Advantages to using a Wired LAN:

- Speed:** Wired LANs almost invariably provide higher speed connections (basically due to the increased reliability).
- Reliability:** Wired LANs tend to be much more reliable as they have a dedicated wire, suitably insulated, down which the router or server can converse with any clients.
- Better Security:** It's more difficult to tap into a (suitably secured) wired LANs than a wireless one as there is no airborne signal that can be picked up.
- Energy Saving:** Less electricity is consumed if your router can send a stream of electrons down a wire instead of having to broadcast on the airwaves.

Disadvantages of Wired LAN:

- Difficult to Physical Setup:** Wired LANs require cables to be installed between your router, hub, switch, printer and computers location(s).
- Security Problems:** Wired LANs may well require more stringent security setup in order to secure them properly.

- 3. **Mobility:** Wired LANs do not provide wireless mobility.
- 4. **Cost:** High cost because of the cost of cables, hub, connectors etc.
- 5. **Time Consuming:** Ethernet cables must be run from each computer to another computer or to the central device like hub or switch. It can be time-consuming and difficult to run cables under the floor or through walls, especially when computers sit in different rooms.

2.6.1 Standard Ethernet

(April 16, 18; Oct. 18)

- The original Ethernet was developed in 1976 at Xerox's Palo Alto Research center (PARC). The original Ethernet technology with the data rate of 10 Mbps refer to the standard Ethernet.
- Ethernet is a standardized system for connecting computers to a Local Area Network (LAN). The Institute for Electrical and Electronic Engineers (IEEE) developed an Ethernet standard known as IEEE Standard 802.3.
- The Standard 802.3 defines rules for configuring an Ethernet network and also specifies how the elements in an Ethernet network interact with one another.
- The 802.3 standard defines rules for configuring an Ethernet network and also specifies how the elements in an Ethernet network interact with one another.
- Since then, it has gone through four generations i.e., Standard Ethernet (10 Mbps), Fast Ethernet (100 Mbps), Gigabit Ethernet (1 Gbps) and Ten-Gigabit Ethernet (10 Gbps) as shown in Fig. 2.44.

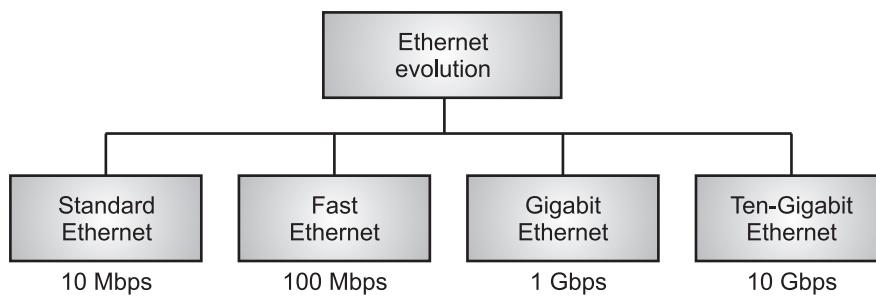


Fig. 2.44: Four generations of Ethernet evolution

2.6.1.1 Characteristics

- Some characteristics of the Standard Ethernet are explained below:
1. **Connectionless and Unreliable Service:**
 - Ethernet provides a connectionless service which means each frame sent is independent of the previous or next frame.
 - Ethernet has no connection establishment or connection termination phases. The sender sends a frame whenever it has it; the receiver may or may not be ready for it.

- The sender may overwhelm the receiver with frames, which may result in dropping frames. If a frame drops, the sender will not know about it.
- Since IP, which is using the service of Ethernet, is also connectionless, it will not know about it either. If the transport layer is also a connectionless protocol, such as UDP, the frame is lost and salvation may only come from the application layer.
- However, if the transport layer is TCP, the sender TCP does not receive acknowledgement for its segment and sends it again.

2. Unreliable Service:

- Ethernet is also unreliable like IP (Internet Protocol) and UDP (User Datagram Protocol).
- If a frame is corrupted during data transmission and the receiver finds out about the corruption, which has a high level of probability of happening because of the CRC-32, the receiver drops the frame silently. It is the duty of high-level protocols to find out about it.

3. Frame Format:

(April 18; Oct., 18)

- The format of the Ethernet MAC frame is shown in Fig. 2.45, and it contains several fields.
- Ethernet does not provide any mechanism for acknowledgment of received frames. Acknowledgments must be implemented at the higher layers.

Preamble : 56 bits of alternating 1s and 0s.

SFD : Start frame delimiter, flag (10101011)

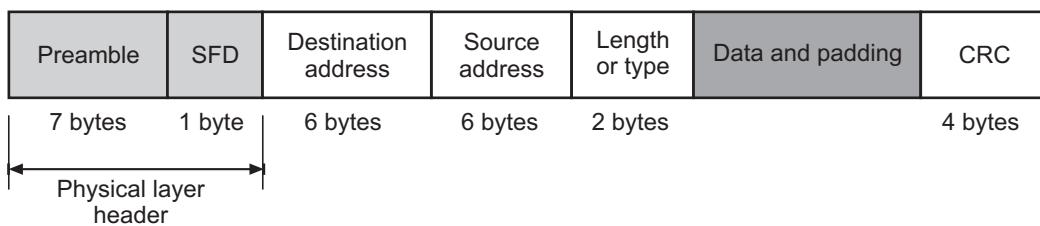


Fig. 2.45: 802.3 Ethernet MAC Frame

- The fields in the frame format are:
 - Preamble:** This is the first field of the 802.3 frame, which contains 7 bytes (56 bits) of alternating 0s and 1s. Which indicates the receiving system about the coming frame and enables it to synchronize its input timing. The preamble is actually added at the physical layer.
 - Start Frame Delimiter (SFD):** SFD is the second field in the frame. Size of this field is 1 byte (1 byte : 10101011). This field signals the beginning of the frame.

The SFD warns the station or stations that this is the last chance for synchronization. The last 2 bits is 11 and alerts the receiver that the next field is the destination address.

- (iii) **Destination Address (DA):** The DA field is of 6 bytes and contains the physical address of the destination station or stations to receive the packet.
- (iv) **Source Address (SA):** The source address field is also 6 bytes and contains the physical address of the sender of the packet.
- (v) **Length or type:** This field is defined as a type field or length field. Both uses are common. The original Ethernet used this field as the type field to define the upper-layer protocol using the MAC frame. The IEEE standard used it as the length field to define the number of bytes in the data field.
- (vi) **Data:** This field contains data encapsulated from the upper-layer protocols. Size of data is minimum of 46 and a maximum of 1500 bytes.
- (vii) **CRC:** This last field contains error detection information.

4. Frame Length:

- Ethernet has forced restrictions about both the minimum and maximum lengths of a frame, as shown in Fig. 2.46.

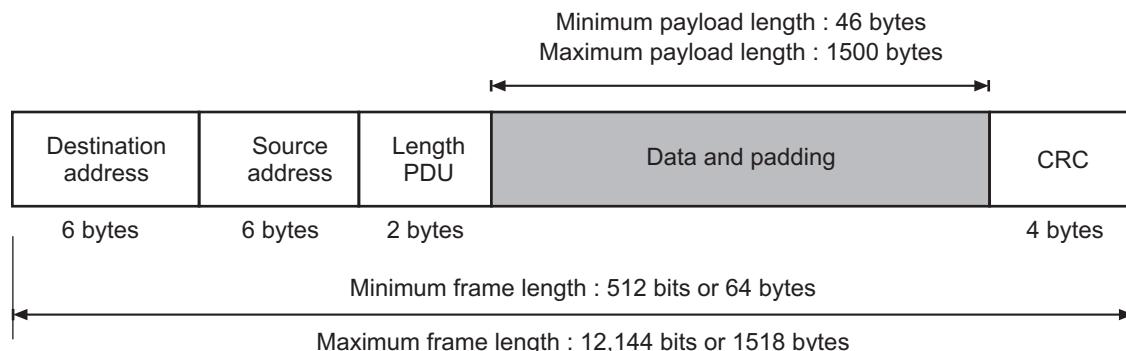


Fig. 2.46: Minimum and Maximum of Ethernet Frame

- As we know CSMA/CD is used as an access protocol in Ethernet.
- The minimum length restriction is required for the correct operation of CSMA/CD. Minimum length of the Ethernet frame is 512 bits or 64 bytes.
- Frame contains 6 bytes of source address, 6 bytes of destination address, 2 bytes of length or type, and 4 bytes of CRC, total 18 bytes of header and trailer are required.
- The minimum length of data from the upper layer is $64 - 18 = 46$ bytes. If the upper layer packet is less than this, padding (adding extra bits) is done.
- The maximum length of an Ethernet frame without preamble and SFD field defined by standard is 1518 bytes.

- If we subtract the 18 bytes of header and trailer, the maximum length of the payload is 1500 bytes.
- The maximum length restriction has following two reasons:
 - (i) Memory was very expensive when Ethernet was designed, this restriction helped to reduce the size of the buffer.
 - (ii) The maximum length restriction prevents one station from taking the complete control of the shared medium, blocking other stations that have data to send.

2.6.2 Addressing

- Every station on an Ethernet network like a PC, workstation, printer etc., has its own Network Interface Card (NIC), installed inside the station.
- The NIC provides the station with a 6-byte (48 bit) physical address. Fig. 2.47 shows physical address in hexadecimal notation.

06 : 01 : 02 : 01 : 2C : 4B
 6 bytes = 12 hex digits = 48 bits

Fig. 2.47: Physical Address in Hexadecimal Notation

Unicast, Multicast and Broadcast Addresses:

- As we know a source address is always a unicast address. The frame comes from only one station. But the destination address can be unicast, multicast or broadcast.
- Fig. 2.48 shows the difference between a unicast address and a multicast address.
- If the least significant bit of the first byte in a destination address is 0, the address is unicast; otherwise, it is multicast.

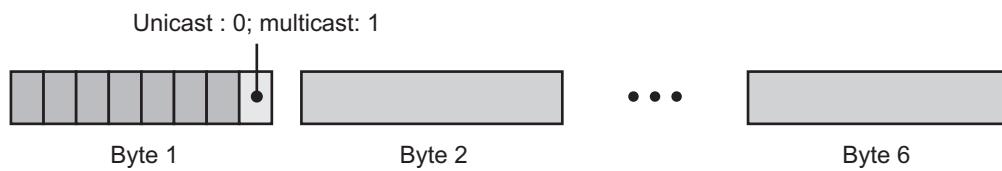


Fig. 2.48: The difference between Unicast Address a Multicast Address

- The broadcast address is a special case of the multicast address i.e. the recipients are all the stations on the LAN. A broadcast destination address contains all forty-eight (48) bits are 1s.

2.6.3 Access Method: CSMA/CD

(April 18)

- Standard Ethernet uses 1-persistent CSMA/CD (Carrier Sense Multiple Access/Collision Detection). 1-persistent mode waits for the medium to be idle, then transmits data.

- CSMA/CD is a type of contention protocol that defines how to respond when a collision is detected, or when two devices attempt to transmit packages simultaneously.
- In an Ethernet network, slot time is defined in bits. It is the time required for a station to send 512 bits. For example, for traditional 10mbps LAN it is 51.2 μ s and calculated as follows

$$\text{Slot time} = \text{Round-trip Time} + \text{Time required to send the Jam Sequence}$$

Slot Time and Collision:

- A 512 bits slot time allows proper functioning of CSMA/CD. To understand this let us consider two cases.

Case 1:

- In the first case, the sender sends a minimum size packet of 512 bits. Before the sender can send the entire packet out, the signal travels through the network and reaches the end of the network.
- If there is another signal at the end of the network collision occurs. The sender can send a jam signal to abort the sending of a frame.
- The round trip time plus the time required to send the jam signal should be less than the time needed for the sender to send the minimum frame, 512 bits.

Case 2:

- The sender must be aware of the collision before it has sent the entire frame.
- In the second case, if the sender sends a frame larger than the minimum size, after sending the first 512 bits, it is guaranteed that collision will not occur during the transmission of this frame.
- The entire medium belongs to the sender. The sender needs to listen for a collision only during the time the first 512 bits are sent.

Slot Time and Maximum Network Length:

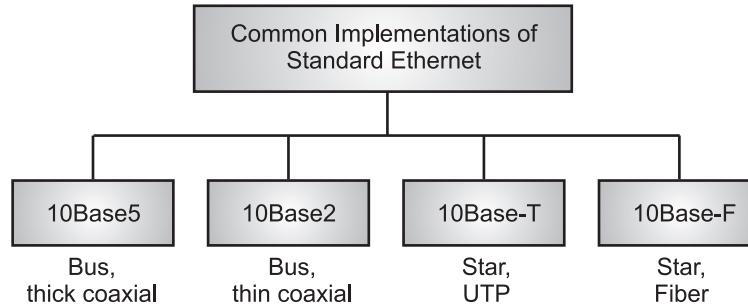
- A relationship between the slot time and maximum length of the network is dependent on the propagation speed of the signal in the particular medium.

$$\text{Max Length} = \text{Propagation Speed} \times \text{Slot Time}/2$$

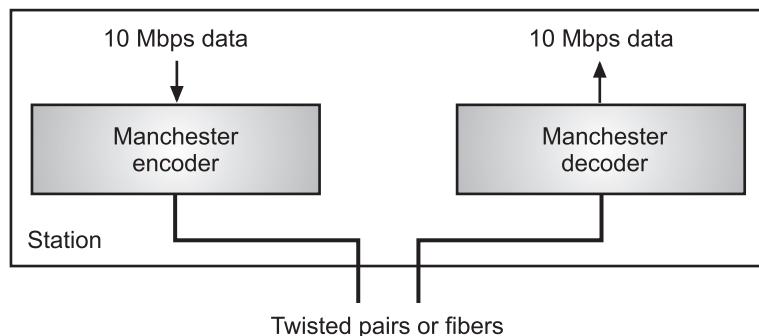
2.6.4 Implementations

(April 19)

- The four common Standard Ethernet implementations during the 1980s are shown in Fig. 2.49.
- In Standard Ethernet implementation (10 Mbps) sender converts data into a digital signal by using the Manchester scheme, at the receiver, received signals are interpreted as Manchester and decoded into data.

**Fig. 2.49: Categories of Standard Ethernet**

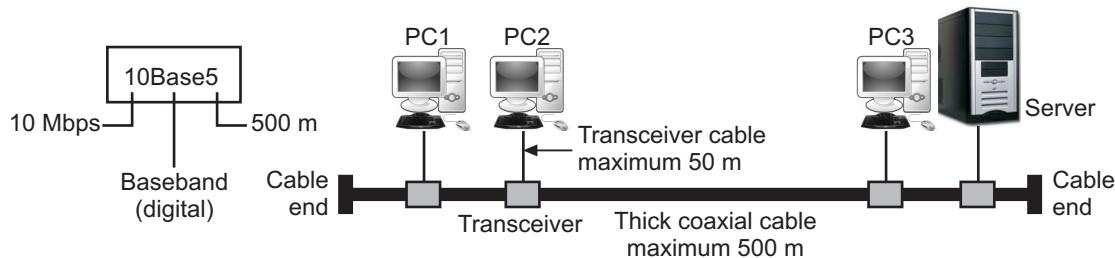
- Fig. 2.50 shows the encoding scheme for Standard Ethernet.

**Fig. 2.50: The encoding scheme for Standard Ethernet**

1. 10Base5 (Thick Ethernet):

(April 19)

- The first Ethernet implementation is called 10Base5, thick Ethernet, or Thicknet. 10Base5 was the first Ethernet specification used in bus topology.
- In 10Base5 specification external transceivers (transmitter and receiver) connected via a tap of a thick coaxial cable.
- Fig. 2.51 shows 10base5 implementation.

**Fig. 2.51: 10Base5 Implementation**

- The transceiver transmits, receives and detects collision. The transceiver is connected to a station via transceiver cable which provides a separate path for sending and receiving. Collision can occur only in the coaxial cable.
- In 10Base5 implementation, the maximum length of coaxial cable should not exceed 500 m, otherwise, signal quality is degraded. If cable length is required more than 500 m, a connecting device repeater is used.

2. 10Base2 (Thin Ethernet):

(April 19)

- The second implementation is called 10Base2, thin Ethernet, or Cheapernet. The 10Base2 also uses a bus topology, it is more cost effective than 10Base5.
- The cable used in this implementation is much thinner, more flexible and can be bent. Due to this cable can pass very close to the stations.
- The transceivers are built inside the Network Interface Card (NIC), which is installed inside the station.
- Thin coaxial is cheaper than thick and the tee (T) connectors are also cheaper than taps used in 10Base5.
- Installation of 10Base2 is simpler because the thin coaxial cable is very flexible. The length of each segment cannot exceed 185 m (close to 200 m) due to the high level of attenuation in thin coaxial cable.
- Fig. 2.52 shows the schematic diagram of a 10Base2 implementation.

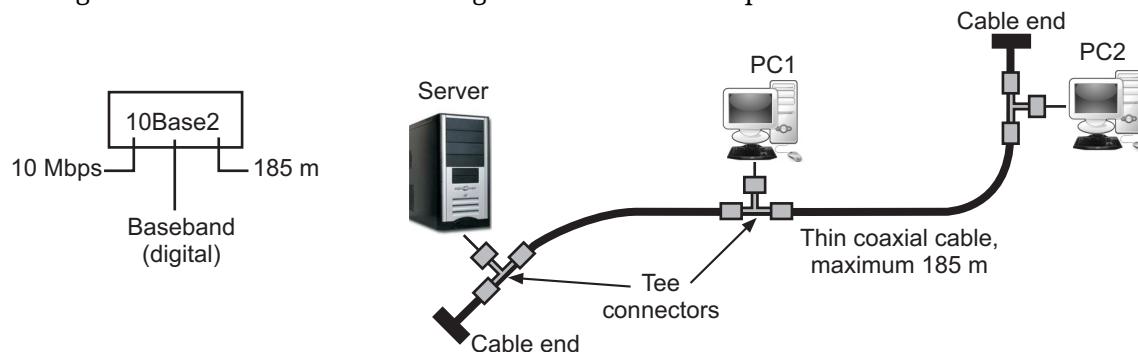


Fig 2.52: 10Base2 Implementation

3. 10Base-T (Twisted-Pair Ethernet):

(April 19)

- The third implementation is 10Base-T or twisted-pair Ethernet. 10Base-T uses physical star topology.
- All stations are connected to a hub or switch via two pairs of twisted pair. From these two pairs one pair is used for sending and other is used for receiving data in between the station and the hub.
- To minimize the effect of attenuation in the twisted pair, its length is defined as 100 m only.

- Fig. 2.53 shows 10Base-T Ethernet implementation.

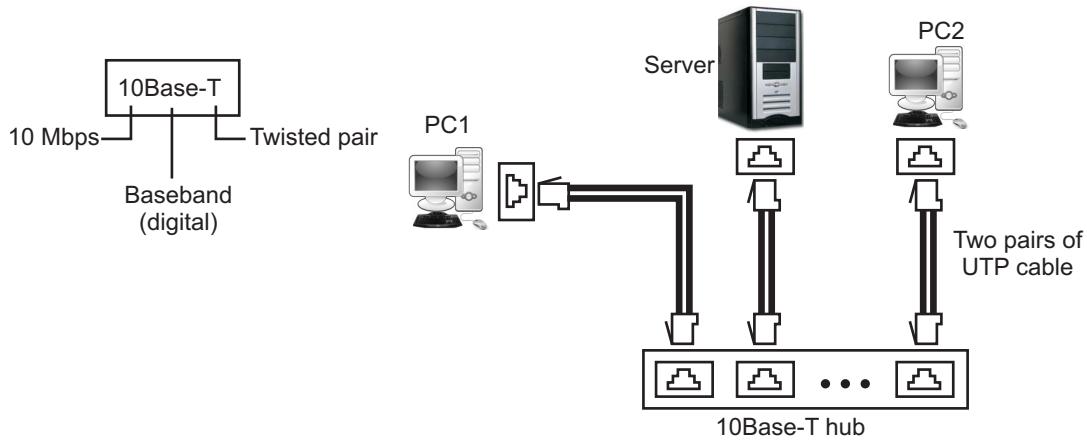


Fig. 2.53: 10Base-T Implementation

(April 19)

4. 10Base-F (Fiber Ethernet):

- 10Base-F uses a star topology to connect stations to a hub.
- The stations are connected to the hub using two fiber-optic cables as shown in the Fig. 2.54.

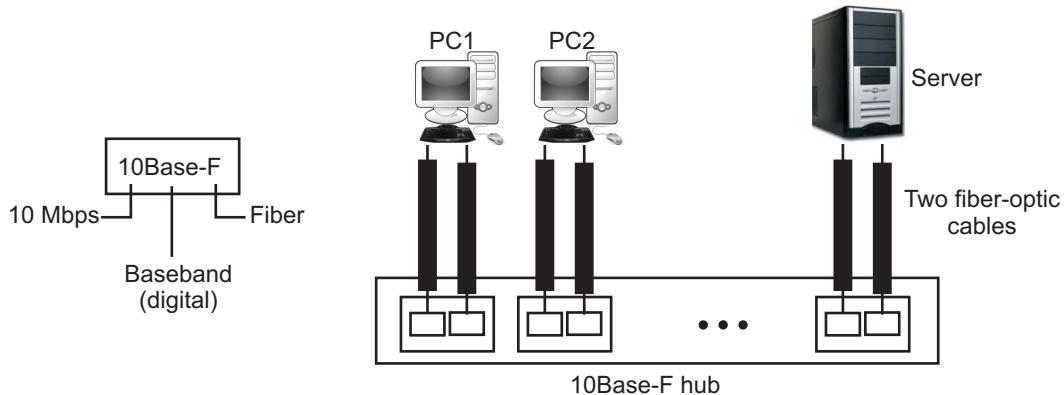


Fig. 2.54: 10Base-F Implementation

Summary of Standard Ethernet Implementation:

Sr. No.	Characteristics	10Base5	10Base2	10Base-T	10Base-F
1.	Media	Thick coaxial cable	Thin coaxial cable	2 UTP	2 Fiber
2.	Maximum length	500 m	185 m	100 m	2000 m
3.	Line encoding	Manchester	Manchester	Manchester	Manchester

2.6.5 Fast Ethernet

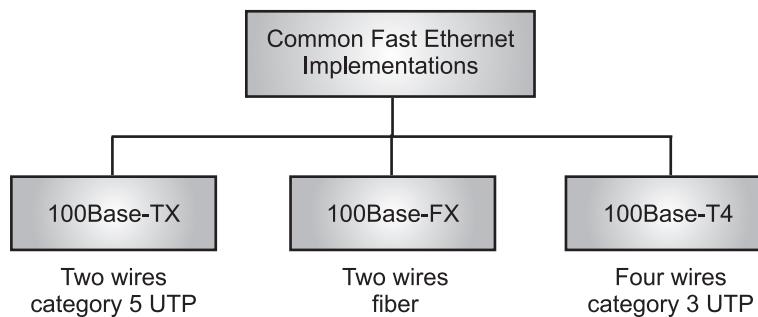
(April 15, 16)

- Fast Ethernet is an Ethernet standard for 100-Mbps data transmission defined by the IEEE 802.3u specification.
- Fast Ethernet was designed to compete with LAN protocols such as FDDI or Fiber Channel.
- Fast Ethernet is 10 times faster than standard Ethernet and operates at 100 Mbps. Fast Ethernet is backward compatible to standard Ethernet.

Goals of Fast Ethernet:

(April 16)

1. Upgrade the data rate to 100 Mbps.
 2. Keep the same 48-bit address.
 3. Make it compatible with Standard Ethernet.
 4. Keep the same frame format.
 5. Keep the same minimum and maximum frame length.
- Autonegotiation is a new feature added to Fast Ethernet. Autonegotiation allows a station or a hub a range of capabilities. It allows two devices to negotiate the mode or data rate of operation. CSMA/CD is an access method used by Fast Ethernet.
 - Fig. 2.55 shows common Fast Ethernet implementation techniques.
 - Fast Ethernet implementation at the physical layer can be categorized as either two-wire or four-wire.
 1. The two-wire implementation can be either category 5 UTP (100Base-TX) or fiber-optic cable (100Base-FX).
 2. The four-wire implementation is designed only for category 3 UTP (100Base-T4).

**Fig. 2.55: Common Fast Ethernet Implementation Techniques**

- Fast Ethernet implementation at the physical layer can be categorized as either two-wire or four-wire.

- Manchester encoding scheme needs a 200-Mbaud bandwidth for a data rate of 100 Mbps.
- Three different encoding schemes are used for three different implementations, as shown in Fig. 2.56.
 1. **100Base-TX:** It uses two pairs of twisted-pair cable (either category 5 UTP or STP). For this implementation, the MLT-3 scheme was used. It supports a data rate of 125 Mbps.
 2. **100Base-FX:** It uses two pairs of fiber-optic cables. 4B/5B encoding is used for this. It supports 100 to 125 Mbps, which can easily be handled by fiber-optic cable.
 3. **100Base-T4:** It was designed to use category 3 or higher UTP. The implementation uses four pairs of UTP for transmitting 100 Mbps. 8B/6T encoding scheme was used. This means that 100 Mbps uses only $(6/8) \times 100$ Mbps, or 75 Mbaud.

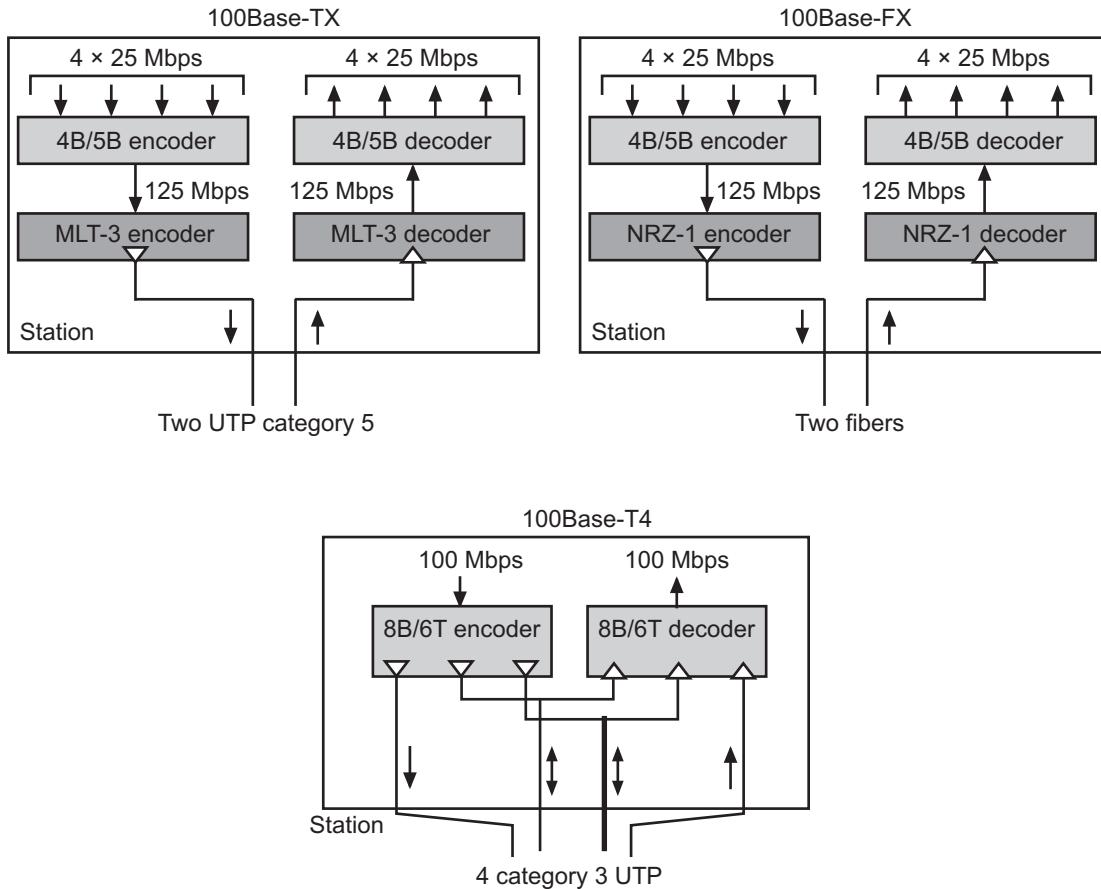


Fig. 2.56: Three different Encoding Schemes

Summary of the Fast Ethernet Implementations:

Sr. No.	Characteristics	100Base-TX	100Base-FX	100Base-T4
1.	Media	Cat 5 UTP or STP	Fiber	Cat 4 UTP
2.	Number of wires	2	2	4
3.	Maximum length	100 m	185 m	100 m
4.	Block encoding	4B/5B	4B/5B	Two 8B/6T
5.	Line encoding	MLT-3	NRZ-I	

Advantages of Fast Ethernet:

1. The performance of Fast Ethernet is 10 times more than in traditional Ethernet.
2. Fast Ethernet is easy to set up.
3. Faster throughput for video, multimedia, graphics, Internet surfing, and other speed-intensive applications.
4. Fast Ethernet supports stronger error detection and correction.
5. Fast Ethernet is ten times faster (100Mbps) than regular 10BaseT networks (10Mbps).

2.6.6 Gigabit Ethernet

- The IEEE initial standard for Gigabit Ethernet was produced by the IEEE in June 1998 as IEEE 802.3z.
- Gigabit Ethernet operates at 1000 Mbps and supports full-duplex (uses central switch) and half-duplex approaches (uses CSMA/CD) for medium access.
- Gigabit Ethernet was developed to meet the need for faster communication networks with applications such as multimedia and Voice over IP (VoIP).

Goals of Gigabit Ethernet:

- 1. Upgrade the data rate to 1 Gbps.
- 2. Make it compatible with Standard of Fast Ethernet.
- 3. Use the same 48-bit address.
- 4. Keep the same minimum and maximum frame length.
- 5. Keep the same frame format.
- 6. To support auto negotiation same as Fast Ethernet.
- Gigabit Ethernet implementations are shown in Fig. 2.57. Two different implementations of Gigabit Ethernet are two wires and a four Wire.
 - 1. The two-wire implementations use fiber-optic cable (1000Base-SX, short-wave, or 1000Base-LX, long-wave), or STP (1000Base-CX).

2. The four-wire version uses category 5 twisted-pair cable (1000Base-T).

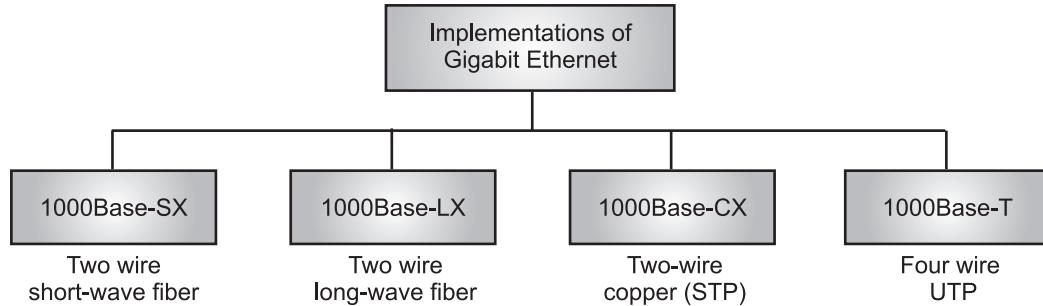


Fig. 2.57: Gigabit Ethernet Implementations

- Fig. 2.58 shows the encoding/decoding schemes for the four wire implementations of Gigabit Ethernet.

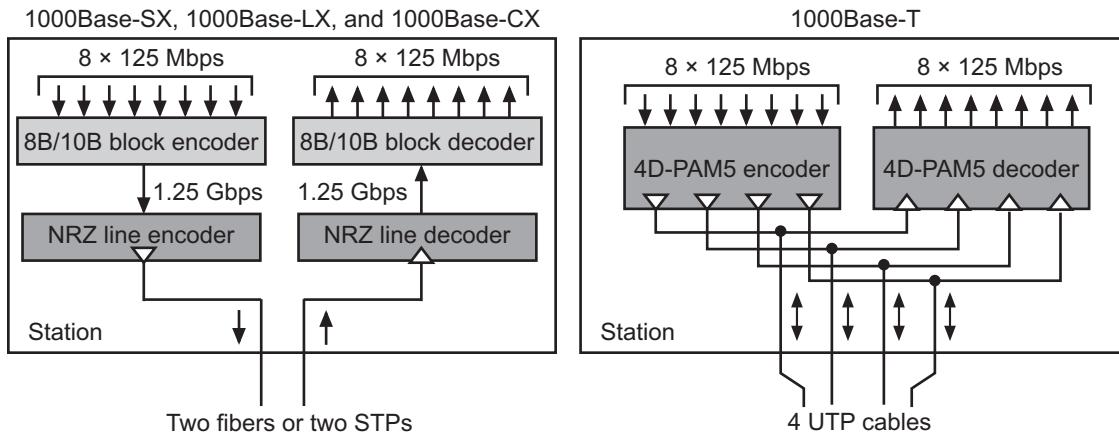


Fig. 2.58: The Encoding/Decoding schemes for the Four Wire Implementations

- Gigabit Ethernet uses 8B/10B block encoding, resulting in 1.25 Gbps.
- In the four-wire implementation, 4D-PAM5 encoding is used to reduce the bandwidth. Thus, all four wires are involved in both input and output; each wire carries 250 Mbps, which is in the range for category 5 UTP cable.

Summary of Gigabit Ethernet Implementation:

Sr. No.	Characteristics	1000Base-SX	1000Base-LX	1000Base-CX	1000Base-T
1.	Media	Fiber short wave	Fiber long wave	STP	Cat 5 UTP
2.	Number of wires	2	2	2	4

Contd...

3.	Maximum length	550 m	5000 m	25 m	100 m
4.	Block encoding	8B/10B	8B/10B	8B/10B	
5.	Line encoding	NRZ	NRZ	NRZ	4D-PAM5

Advantages of Gigabit Ethernet:

1. It is roughly 100 times faster than the regular Mbps Ethernet.
2. The elimination of bottlenecks within the Internet service.
3. Improving the traffic flow in overcrowded areas.
4. Transferring large amounts of data across a network quickly.
5. Gigabit Ethernet cables are easier to install and setup.
6. Gigabit Ethernet offers performance enhancement for existing networks without having to change the cables, protocols and applications already in use.
7. Gigabit Ethernet cable may be a cheaper option than optical fiber.

Disadvantages of Gigabit Ethernet:

1. It is rather expensive.
2. The amount of bandwidth we have is not guaranteed.

Differences between Fast Ethernet and Gigabit Ethernet:

Sr. No.	Key	Fast Ethernet	Gigabit Ethernet
1.	Successor	Fast Ethernet is the successor of 10-Base-T-Ethernet.	Gigabit Ethernet is the successor of Fast Ethernet.
2.	Network speed	Fast Ethernet speed is upto 100 Mbps.	Gigabit Ethernet speed is upto 1 Gbps.
3.	Complexity	Fast Ethernet is simple to configure.	Gigabit Ethernet is quiet complex to configure.
4.	Delay	Fast Ethernet generates more delay.	Gigabit Ethernet generates less delay than Fast Ethernet.
5.	Coverage Limit	Fast Ethernet coverage limit is upto 10KM.	Gigabit Ethernet coverage limit is upto 70KM.
6.	Round trip delay	Fast Ethernet round trip delay is 100 to 500 bit times.	Gigabit Ethernet round trip delay is 4000 bit times.

2.7 WIRELESS LANs

(Oct. 17)

- Today, wireless communication is one of the fastest growing technologies. The demand for connecting devices without the use of cables is increasing everywhere.
- Wireless LANs are those Local Area Networks that use high frequency radio waves instead of cables for connecting the devices in LAN.
- A wireless LAN (WLAN) is a wireless computer network that links two or more devices using wireless communication to form a local area network (LAN) within a limited area such as a home, school, computer laboratory, campus, or office building.
- The two types of Wireless LAN are IEEE 802.11 (sometimes called Wireless Ethernet or Wi-Fi), and Bluetooth (sometimes called Personal Area Network (PAN)).
- 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 (AP) for Internet access.

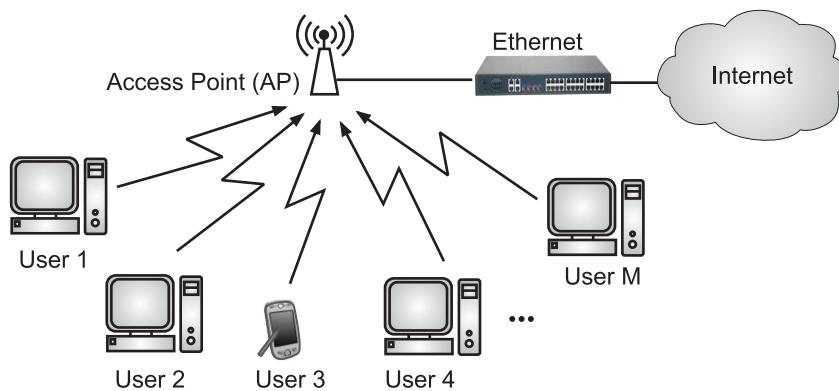


Fig. 2.59: Wireless LAN

Advantages Wireless LAN:

- Convenience:** All notebook computers and many mobile phones are equipped with the Wi-Fi technology to connect directly to a wireless LAN.
- Ease of Setup:** Since, a wireless LAN does not require running physical cables through a location, installation can be quick and cost-effective.
- Scalability:** A wireless LAN can typically expand with existing equipment, while a wired network might require additional cables and other materials.
- Security:** Controlling and managing access to the wireless LAN is important to its success. WLANs provide robust security protection, so the data is easily available to only those users to allow authorised access.

5. **Cost:** It can cost less to operate a wireless LAN, which eliminates or reduces wiring costs during office moves, reconfigurations, or expansions.
6. **Mobility:** Mobility is a significant advantage of WLANs. Users can access shared resources without looking for a place to plug in, anywhere in the organization. A wireless network allows users to be truly mobile as long as the mobile terminal is under the network coverage area.

Disadvantages of Wireless LAN:

1. **Speed:** The speed on most wireless LAN networks (typically 1-108 Mbit/s) is reasonably slow.
2. **Security:** Wireless LAN are much more susceptible to unauthorized use.
3. **Interference:** Because wireless LANs use radio signals and similar techniques for transmission, they are susceptible to interference from lights and electronic devices.
4. **QoS :** WLAN offers typically lower QoS. Lower bandwidth due to limitations in radio transmission and higher error rates due to interference.

2.7.1 Architectural Comparison

- In this section, we compare the architecture of wired and wireless LANs to give some idea of what we need to look for when we study wireless LANs.
1. **Medium:**
 - In a wired LAN, we use wires/cables to connect hosts. We moved from multiple access to point-to-point access through the generation of the Ethernet.
 - In a wireless LAN, the medium is air, the signal is generally broadcast. When hosts in a wireless LAN communicate with each other, they are sharing the same medium (multiple access).
 2. **Host:**
 - In a wired LAN, a host is always connected to its network at a point with a fixed link layer address related to its Network Interface Card (NIC).
 - A host can move from one point in the Internet to another point. In this case, its link-layer address remains the same, but its network-layer address will change.
 - However, before the host can use the services of the Internet, it needs to be physically connected to the Internet.
 - In a wireless LAN, a host is not physically connected to the network; it can move freely and can use the services provided by the network.
 - Therefore, mobility in a wired network and wireless network are totally different issues.

3. Connected to other Networks:

- A wired LAN can be connected to another network or an internetwork such as the Internet using a router.
- A wireless LAN may be connected to a wired infrastructure network, to a wireless infrastructure network, or to another wireless LAN.
- Fig. 2.60 shows the two environments of a wired LAN and a wireless LAN.

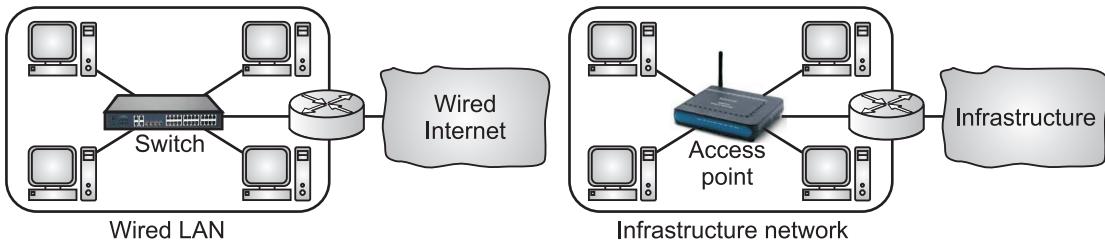


Fig. 2.60: Connection of a Wired and a Wireless LAN to other Networks

- In this case, the wireless LAN is referred to as an infrastructure network and the connection to the wired infrastructure, such as the Internet, is done via a device called an Access Point (AP).
- An AP is gluing two different environments together namely, one wired and one wireless.
- Communication between the AP and the wireless host occurs in a wireless environment while communication between the AP and the infrastructure occurs in a wired environment.

4. Isolated LANs:

- The concept of a wired isolated LAN also differs from that of a wireless isolated LAN. A wired isolated LAN is a set of hosts connected via a link-layer switch (in the recent generation of Ethernet).
- A wireless isolated LAN, called an ad hoc network in wireless LAN terminology, is a set of hosts that communicate freely with each other.

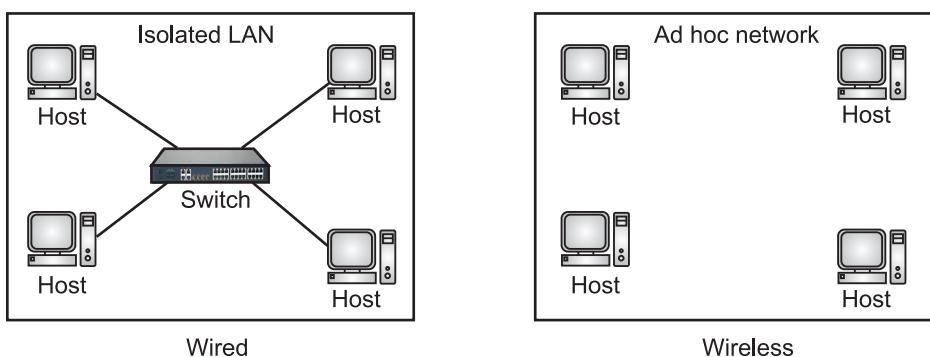


Fig. 2.61: Isolated LANs (Wired vs Wireless)

- The concept of a link-layer switch does not exist in wireless LANs. Fig. 2.61 shows two isolated LANs, one wired and one wireless.

5. Moving between Environments:

- A wired LAN or a wireless LAN operates only in the lower two layers of the TCP/IP protocol suite.
- Means that if we have a wired LAN in a building that is connected via a router or a modem to the Internet, all we need in order to move from the wired environment to a wireless environment is to change the network interface cards designed for wired environments to the ones designed for wireless environments and replace the link-layer switch with an access point.
- In this change, the link-layer addresses will change (because of changing NICs), but the network-layer addresses (IP addresses) will remain the same; we are moving from wired links to wireless links.

2.7.2 Characteristics

- There are a number of characteristics of wireless LANs that either do not apply to wired LANs or the existence of which is negligible and can be ignored.

- Some of these characteristics are explained below:

1. Interference:

- The main issue is that a receiver may receive signals not only from the intended sender, but also from other senders if they are using the same frequency band.

2. Attenuation:

- The strength of electromagnetic signals decreases rapidly because the signal disperses in all directions; only a small portion of it reaches the receiver.
- The situation becomes worse with mobile senders that operate on batteries and normally have small power supplies.

3. Error:

- The errors and error detection are more serious issues in a wireless network than in a wired network.

4. Multipath Propagation:

- A receiver may receive more than one signal from the same sender because electromagnetic waves can be reflected back from obstacles such as walls, the ground, or objects.
- The result is that the receiver receives some signals at different phases (because they travel different paths). This makes the signal less recognizable.

2.7.3 Access Control

- In wireless LAN, CSMA/CD cannot be implemented because of following reasons:
 1. For collision detection, a station must be able to send data and receive collision signals at the same time, which increases bandwidth requirements.
 2. Collisions may not be detected because of the hidden station problem.
 3. The distance between stations can be great. Signal fading could prevent a station at one end from hearing a collision at the other end.
- To overcome the above three problems, Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) was invented for wireless LANs.
- Fig. 2.62 shows data exchange and control frames used in CSMA/CA. Before sending a frame, the source station senses the medium. There are two options:
 1. The channel uses a persistence strategy with back-off until the channel is idle.
 2. After the station is found to be idle, the station waits for a period of time called the Distributed InterFrame Space (DIFS), then the station sends a control frame Request To Send (RTS).
- After receiving the RTS and waiting for a period Short InterFrame Space (SIFS), the destination sends a control frame called Clear To Send (CTS). This control frame indicates to source that the destination station is ready to receive data.
- The source then waits for time equal to SIFS and then sends data. After receiving data, the destination waits for time equal to SIFS and sends acknowledgement to the source.

Network Allocation Vector (NAV):

- It's interesting to see how the collision avoidance is handled by the protocol. CSMA/CA protocol uses a feature called NAV.
- When a station sends to an RTS frame, it also includes the total time that is needed to occupy the channel.
- The stations that are affected by this transmission create a timer called NAV, that shows how much time these stations should not sense the channel.
- Each time a station accesses the system and sends to an RTS frame, another station starts NAV.
- Two or more stations may try to send RTS frames at the same time. These control frames may collide and destroy.

- The sender assumes there has been a collision if it has not received a CTS from the receiver. In such a situation, the sender tries again. This concept is known as collision during handshaking.

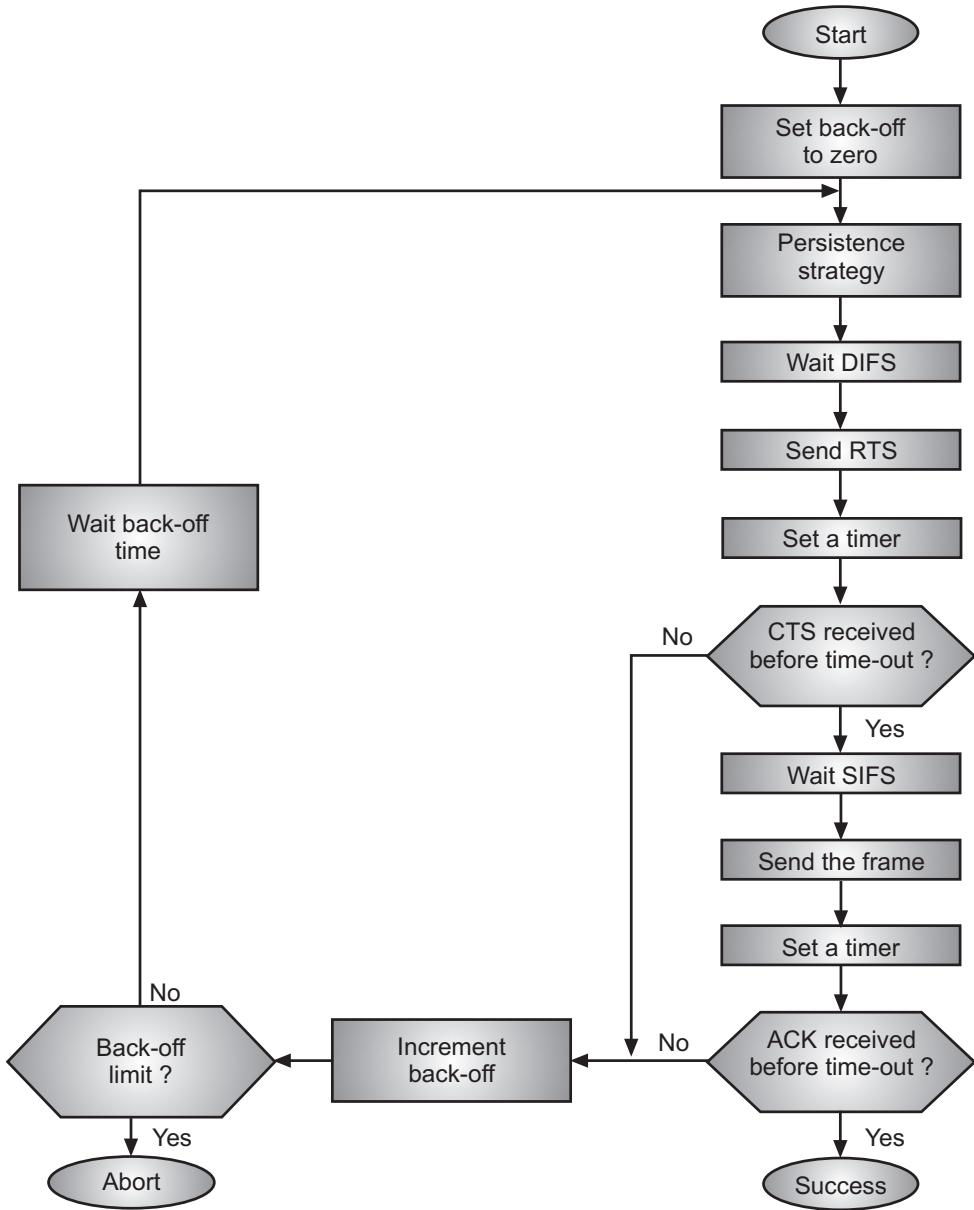


Fig. 2.62: Data Exchange and Control Frames used in CSMA/CA

2.7.4 IEEE 802.11 Architecture

(April 16)

- IEEE defines a standard for wireless LAN, named IEEE 802.11, which covers the physical and data link layers.
- IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which covers the physical and data-link layers.
- It is sometimes called wireless Ethernet. In some countries, including the United States, the public uses the term WiFi (Wireless Fidelity) as a synonym for wireless LAN.
- WiFi however, is a wireless LAN that is certified by the WiFi Alliance, a global, nonprofit industry association of more than 300 member companies devoted to promoting the growth of wireless LANs.
- The IEEE 802.11 standard defines two different services BSS and ESS as explained below:

1. Basic Service Set (BSS):

(April 18; Oct. 18)

- BSS is a building block for a Wireless LAN. A BSS is made up of stationary or mobile wireless station and an optional central base station, known as Access Point (AP).
- The BSS without an AP is a stand-alone network and called as ad hoc architecture. Such types of networks cannot send data to other BSSs.
- Stations can form a network without the need of AP. Stations can locate one another and agree to be part of a BSS.
- A BSS with an AP is called an infrastructure network. All stations in such architecture are communicating through an AP.
- Fig. 2.63 shows two sets of IEEE 802.11 standard.

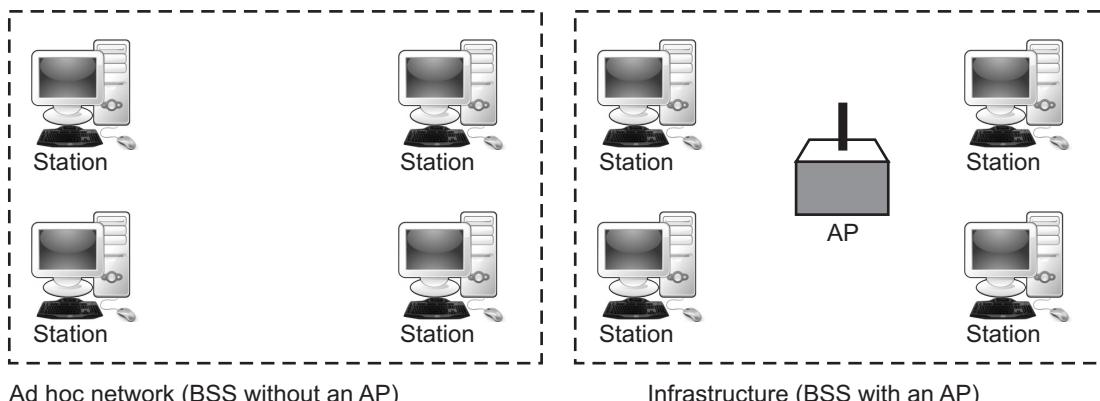
BSS : Basic Service Set**AP** : Access Point

Fig. 2.63: Two Sets of IEEE 802.11 Standard

2. Extended Service Set (ESS):

- An extended service set is made up of two or more BSSs with APs.
- The BSSs are connected through a distribution system, which is a wired LAN. The distribution system connects the APs in the BSSs.
- ESS uses two types of stations, i.e., mobile and stationary stations. The mobile stations are the normal stations in the BSS. The stationary stations are AP stations that are part of a wired LAN.
- Communication between two stations from two different BSSs take place via., two APs. But when stations are within reach of one another, they can communicate directly, without the use of AP.

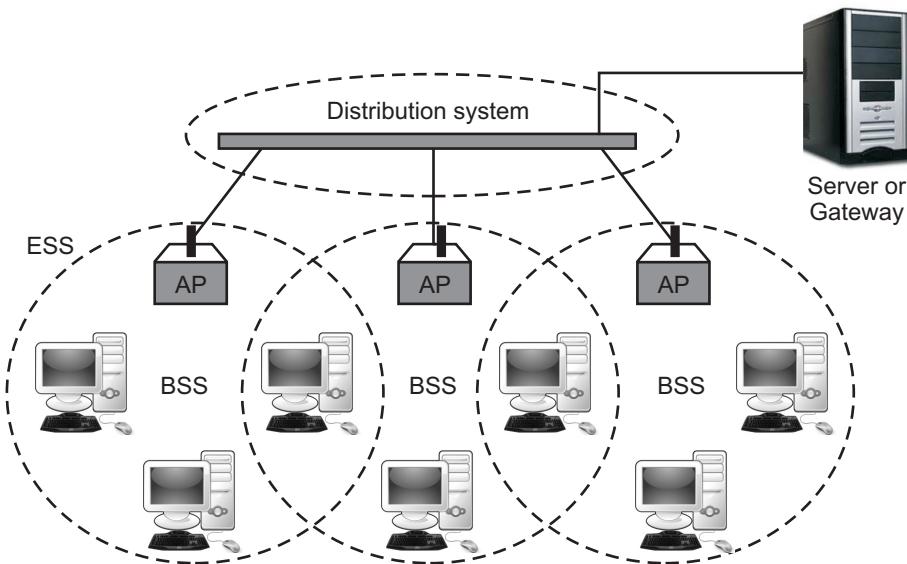


Fig. 2.64: Extended Service Set (ESS)

Station Types:

- Based on mobility, IEEE 802.11 defines three types of stations in a wireless LAN, as given below:
 1. **No-transition:** A station with no-transition mobility is either stationary (not moving) or moving only inside a BSS.
 2. **BSS-transition:** A station with BSS-transition mobility can move from one BSS to another, but the movement is in one ESS only.
 3. **ESS-transition:** A station with ESS-transition mobility can move from one ESS to another.

2.7.5 Physical Layer

(April 18)

- As we know that the physical layer is responsible for converting data streams into signals, the bits of 802.11 networks can be converted to radio waves or infrared waves.
- The 802.11 physical layer (PHY) is the interface between the MAC and the wireless media where frames are transmitted and received.
- The specifications of IEEE 802.11 are explained below:
 - IEEE 802.11 Infrared:**
 - It uses diffused infrared light in the range of 800 to 950 nm. It allows two different speeds 1 Mbps and 2Mbps.
 - For a 1 Mbps data rate, 4 bits of data are encoded into 16 bit code. This 16 bit code contains fifteen 0s and a single 1.
 - For a 2-Mbps data rate, a 2 bit code is encoded into 4 bit code. This 4 bit code contains three 0s and a single 1.
 - The modulation technique used is Pulse Position Modulation (PPM) i.e. for converting digital signal to analog.
 - IEEE 802.11 FHSS:**
 - IEEE 802.11 uses Frequency Hopping Spread Spectrum (FHSS) method for signal generation.
 - The FHSS method uses a 2.4 GHz ISM band. This band is divided into 79 sub-bands of 1MHz with some guard bands.
 - In this method, at one moment data is sent by using one carrier frequency and then by some other carrier frequency at the next moment.
 - After this, idle time is there in communication. This cycle is repeated after regular intervals.
 - In FHSS a pseudo random number generator selects the hopping sequence. The allowed data rates are 1 or 2 Mbps.
 - The FHSS method uses frequency shift keying (two level or four level) for modulation i.e. for converting digital signal to analogy.
 - IEEE 802.11 DSSS:**
 - This method uses Direct Sequence Spread Spectrum (DSSS) method for signal generation. Each bit is transmitted as 11 chips using a Barker sequence.
 - DSSS uses the 2.4-GHz ISM band. It also allows the data rates of 1 or 2 Mbps.
 - It uses Phase Shift Keying (PSK) technique at 1 M baud for converting digital signal to analog signal.

4. IEEE 802.11a OFDM:

- This method uses Orthogonal Frequency Division Multiplexing (OFDM) for signal generation.
- This method is capable of delivering data upto 18 or 54 Mbps. In OFDM all the subbands are used by one source at a given time.
- It uses a 5 GHz ISM band. This band is divided into 52 subbands, with 48 subbands for data and 4 subbands for control information.
- If Phase Shift Keying (PSK) is used for modulation then data rate is 18 Mbps. If Quadrature Amplitude Modulation (QAM) is used, the data rate can be 54 Mbps.

5. IEEE 802.11b HR-DSSS:

- It uses the High Rate Direct Sequence Spread Spectrum method for signal generation.
- HR-DSSS is similar to DSSS except for the encoding method. Here, 4 or 8 bits are encoded into a special symbol called Complementary Code Key (CCK).
- It uses a 2.4 GHz ISM band. It supports four data rates 1, 2, 5.5 and 11 Mbps. 1 Mbps and 2 Mbps data rates use phase shift modulation. The 5.5 Mbps version uses BPSK and transmits at 1.375 Mbaud/s with 4-bit CCK encoding.
- The 11 Mbps version uses QPSK and transmits at 1.375 Mbps with 8-bit CCK encoding.

6. IEEE 802.11g OFDM:

- It uses OFDM modulation technique. It uses a 2.4 GHz ISM band.
- It supports the data rates of 22 or 54 Mbps. It is backward compatible with 802.11 b.

7. IEEE 802.11n:

- An upgrade to the 802.11 project is called 802.11n (the next generation of wireless LAN). The goal is to increase the throughput of 802.11 wireless LANs.
- The new standard emphasizes not only the higher bit rate but also eliminating some unnecessary overhead. The standard uses what is called MIMO (Multiple-Input Multiple-Output antenna) to overcome the noise problem in wireless LANs.

2.7.6 MAC Sublayer

- IEEE 802.11 defines two MAC sublayers, Distribution Coordination Function (DCF) and Point Coordination Function (PCF).
- Fig. 2.65 shows the relationship between the two MAC sublayers, the LLC sublayer and the physical layer.
- CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) is the protocol used to access methods defined by IEEE at the MAC sublayer is called the Distribution Coordination Function (DCF).

- The Point Co-ordination Function (PCF) is an optional access method which is implemented in an infrastructure network and not in an ad hoc network. It is implemented on top of the DCF and is used for time sensitive transmission.

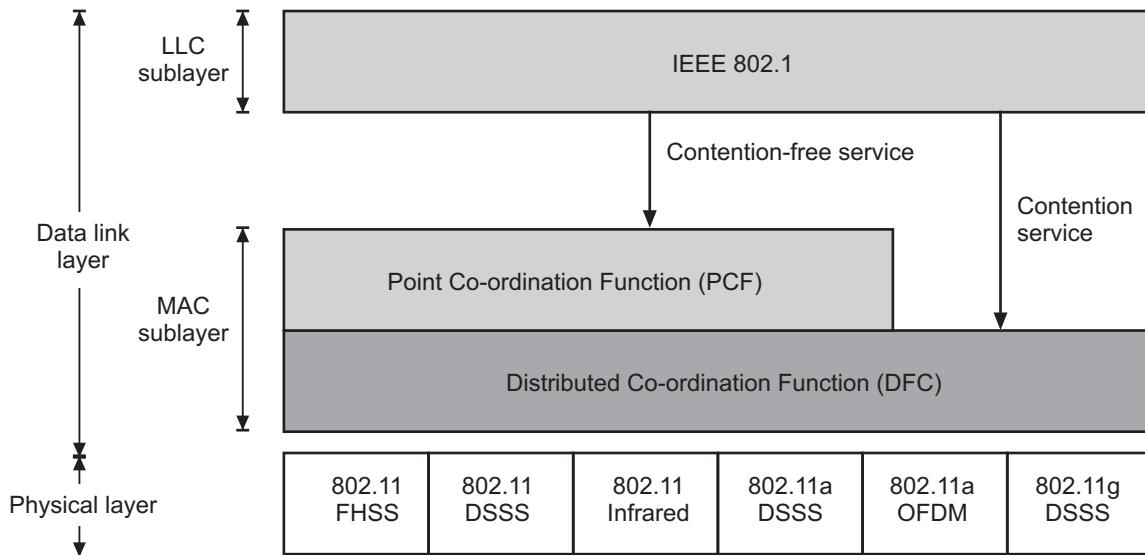


Fig. 2.65: The Relationship between Layers

2.7.6.1 Frame Format

(Oct. 17)

- The MAC layer consists of nine fields as shown in Fig. 2.66.

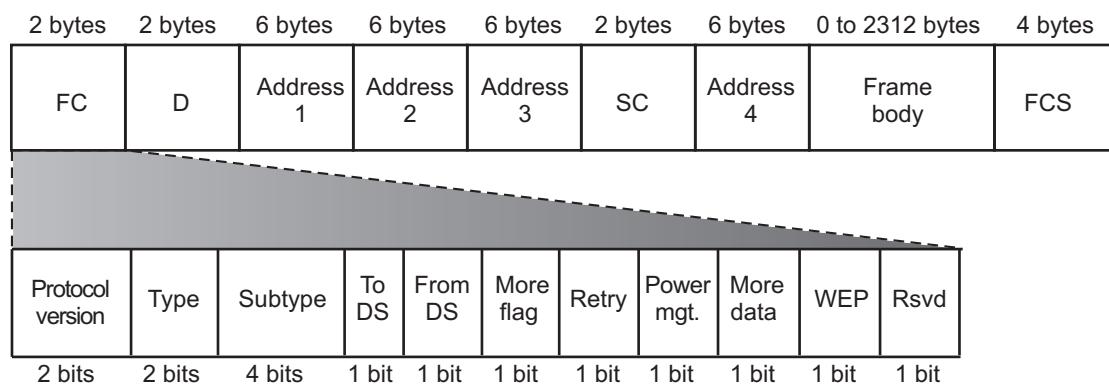


Fig. 2.66: MAC Layer Frame Format

- The MAC layer frame consists of following nine fields:
 - Frame Control (FC):** The FC field is 2 bytes long and defines the type of frame and some control information. The subfields of FC field are listed below:
 - Version:** Current version is 0.

- (ii) **Type:** Type of information: management (00), control (01), or data (10).
 - (iii) **Subtype:** Subtype of each type.
 - (iv) **To DS:** Defined later.
 - (v) **From DS:** Defined later.
 - (vi) **More flag:** When set to 1, means more fragments.
 - (vii) **Retry:** When set to 1, means retransmitted frame.
 - (viii) **Pwr mgt:** When set to 1, means the station is in power management mode.
 - (ix) **More data:** When set to 1, means the station has more data to send.
 - (x) **WEP:** Wired equivalent privacy (encryption implemented).
 - (xi) **Rsvd:** Reserved.
2. **D:** In all frames, this field defines the duration of the transmission that is used to set the value of NAV.
3. **Addresses:** There are four address fields, each 6 bytes long. The meaning of each address field depends on the value of the To DS and From DS subfields.

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	Destination	Source	BSS ID	N/A
0	1	Destination	Sending AP	Source	N/A
1	0	Receiving AP	Source	Destination	N/A
1	1	Receiving AP	Sending AP	Destination	Source

4. **Sequence control:** This field defines the sequence number of the frame to be used in flow control.
5. **Frame body:** This field between 0 to 2312 bytes contains information based on the type and the subtype defined in the FC field.
6. **FCS:** This field is used for error detection.

Frame Types:

- IEEE 802.11, wireless LAN defines three types of frames, as explained below:
 1. **Management Frames:** Management frames are used for the initial communication between stations and access points.
 2. **Control Frames:** Control frames are used for accessing the channel and acknowledging frames.
 3. **Data Frames:** Data frames are used for carrying data and control information.

2.7.7 Bluetooth

(April 17)

- Bluetooth is a wireless LAN technology used to connect devices of different functions such as telephones, computers like laptop or desktop, notebooks, cameras, printers and so on.
- The Bluetooth specifications are developed and licensed by the Bluetooth Special Interest Group.
- Bluetooth technology is a short-range wireless radio technology that allows electronic devices to connect to one another.
- Generally, Bluetooth has a range of up to 30 ft., or greater, depending on the Bluetooth Core Specification Version. Newer devices, using newer versions of Bluetooth, have ranges over 100 ft.
- A Bluetooth LAN is an ad hoc network, which means that the network is formed spontaneously. The devices find each other and make a network.
- Bluetooth is an open specification for short-range wireless transmission of voice and data. It provides a simple, low-cost seamless wireless connectivity between portable handheld devices.
- Bluetooth technology is the implementation of a protocol defined by the IEEE 802.15 standard.
- The standard defines a wireless Personal Area Network (PAN) operable in an area the size of a room or a hall.

2.7.7.1 Bluetooth Architecture

(Oct. 18)

- Bluetooth architecture defines two types of networks i.e., Piconet and Scatternet.
- 1. Piconet:**
- Piconet is a Bluetooth network that consists of one primary (master) node and seven active secondary (slave) nodes.
 - Thus, piconet can have upto eight active nodes (1 master and 7 slaves) or stations within the distance of 10 meters.
 - There can be only one primary or master station in each piconet.
 - The communication between the primary and the secondary can be one-to-one or one-to-many.
 - Fig. 2.67 shows typical piconet. All communication is between master and a slave. Slave-slave communication is not possible.
 - In addition to seven active slave stations, a piconet can have up to 255 parked nodes. These parked nodes are secondary or slave stations and cannot take part in communication until it is moved from parked state to active state.

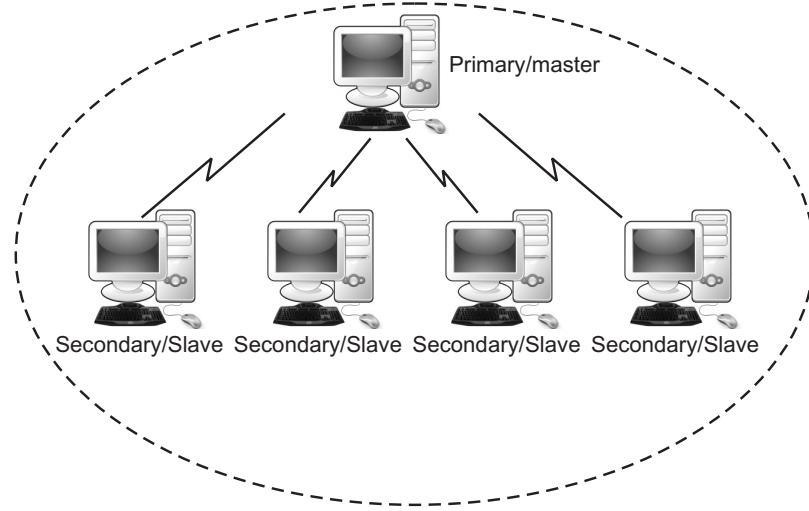


Fig. 2.67: Piconet

2. Scatternet:

(April 18)

- Scatternet is formed by combining various piconets.
- A slave in one piconet can act as a master or primary in another piconet.
- Fig. 2.68 shows scatternet.

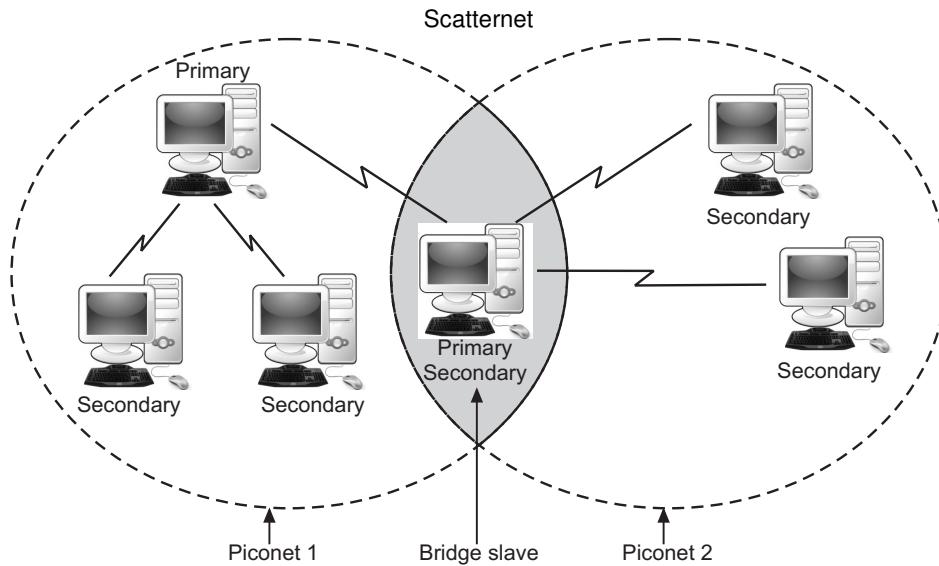


Fig. 2.68: Scatternet

- Such a station or node can receive messages from the master in the first piconet and deliver the message to its slaves in other piconet where it is acting as master. This node is also called bridge slave.

- Thus, a station can be a member of two piconets. A station cannot be a master in two piconets.

2.7.7.2 Bluetooth Layers

- Bluetooth network technology connects mobile devices wirelessly over a short-range to form a Personal Area Network (PAN).
- The Bluetooth architecture, showing all the major layers in the Bluetooth system, are shown in Fig. 2.69.
- The layers below can be considered to be different hurdles in an obstacle course. This is because all the layer's function one after the other. One layer comes into play only after the data has been through the previous layer.

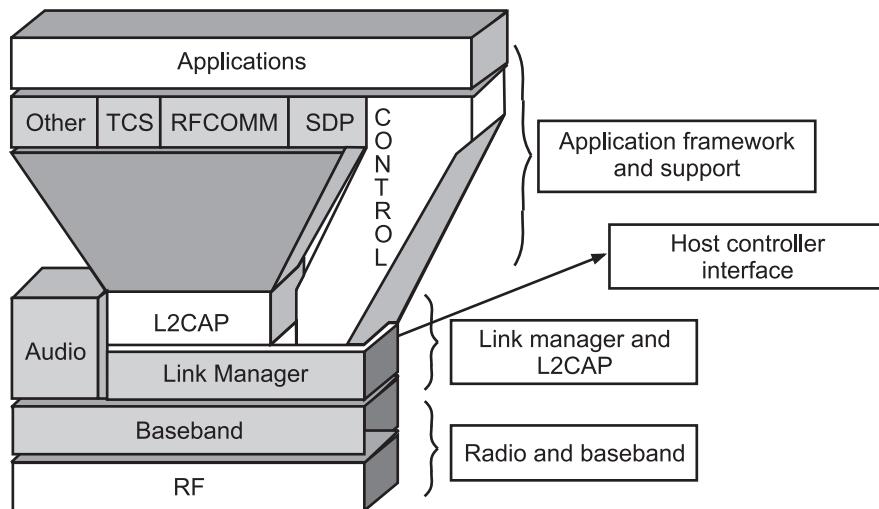


Fig. 2.69: Bluetooth Architecture

- Layers of Bluetooth in Fig. 2.69 are explained below:
 - 1. Radio Frequency (RF)**: The radio frequency layer defines the requirements for a Bluetooth transceiver operating in the 2.4 GHz ISM band.
 - 2. Baseband**: The baseband layer describes the specification of the Bluetooth Link Controller (LC), which carries out the base band protocols and other low-level link routines. It specifies piconet/channel definition, "low-level" packet definition, channel sharing.
 - 3. LMP**: The Link Manager Protocol (LMP) is used by the link managers (on either side) for link set-up and control.
 - 4. HCI**: The Host Controller Interface (HCI) provides a command interface to the baseband link controller and link manager, and access to hardware status and control registers.

5. **L2CAP:** Logical Link Control and Adaptation Protocol (L2CAP) supports higher level protocol multiplexing, packet segmentation and reassembly, and the conveying of quality of service information.
6. **Radio Frequency Communication (RFCOMM):** RFCOMM layer takes care of the communication channel between two devices or between a master and a slave. It connects the serial ports of all the devices according to the requirement.
7. **Service Discovery Protocol (SDP):** This layer provides a means for applications to discover which services are available and to determine the characteristics of those available services.
8. **Telephony Control protocol Specification (TCS):** Basic function of this layer is call control (setup and release) and group management for gateway serving multiple devices.
9. **Application Program Interface (API) Libraries:** These are software modules which connect the host application program to the Bluetooth communications system. As such they reside and execute on the same processing resource as the host system application.

2.7.7.3 Bluetooth Frame Format

- Fig. 2.70 shows the frame format of Bluetooth.

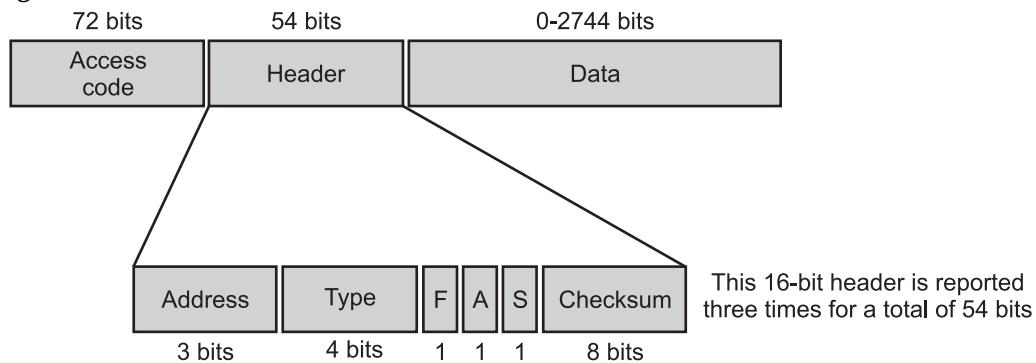


Fig. 2.70

- The various fields of Bluetooth frame format are explained below:
 1. **Access Code:** It is a 72 bit field that contains synchronization bits. It identifies the master.
 2. **Header:** This is a 54-bit field. It contains an 18 bit pattern that is repeated for 3 times. The header field contains following subfields:
 - (i) **Address:** This 3 bit field can define up to seven slaves (1 to 7). If the address is zero, it is used for broadcast communication from primary to all secondaries.

- (ii) **(ii) Type:** This 4 bit field identifies the type of data coming from upper layers.
- (iii) **F:** This flow bit is used for flow control. When set to 1, it means the device is unable to receive more frames.
- (iv) **A:** This bit is used for acknowledgement.
- (v) **S:** This bit contains a sequence number of the frame to detect retransmission. As stop and wait protocol is used, one bit is sufficient.
- (vi) **Checksum:** This 8 bit field contains checksum to detect errors in header.
- 3. **Data:** This field can be 0 to 2744 bits long. It contains data or control information coming from upper layers.

2.7.7.4 Advantages, disadvantages and Applications of Bluetooth

Advantages of Bluetooth:

1. It is cheaper in cost.
2. Easy to install and setup.
3. It makes connecting to different devices convenient.
4. Setting up a Bluetooth connection between two devices is quick and easy.
5. It is wireless technology.
6. Bluetooth doesn't need any configuration to start a connection and perform file transfers.
7. Bluetooth is actually inexpensive.
8. Bluetooth is automatic i.e., when two or more devices enter a range of up to 30 feet of each other, they will automatically begin to communicate without you having to do anything.
9. Bluetooth devices almost always avoid interference from other wireless devices.
10. The standard for Bluetooth will allow compatible devices to share data and voice communications. This is great for mobile phones and headsets.

Disadvantages of Bluetooth:

1. Bluetooth only allows short range communication between devices (less than 10 meters).
2. Bluetooth only offers 1 Mbps to 3 Mbps data transfer rate.
3. Bluetooth makes it much more open to interception and attack. For this reason, security is a very key aspect to the Bluetooth specification.
4. It can lose connection in certain conditions.

Applications of Bluetooth:

(April 17; Oct. 17)

1. It is used for providing communication between peripheral devices like wireless mouse or keyboard with the computer.

2. It is used by modern healthcare devices to send signals to monitors.
3. It is used by modern communicating devices like mobile phones, PDAs, palmtops etc. to transfer data rapidly.
4. It is used for dial up networking. Thus allowing a notebook computer to call via a mobile phone.
5. It is used for cordless telephoning to connect a handset and its local base station.
6. It also allows hands-free voice communication with a headset.
7. It also enables a mobile computer to connect to a fixed LAN.

Difference between Wireless LAN and Bluetooth:

(April 19)

Sr. No.	Bluetooth	Wireless LAN
1.	It is a short range technology standard which allows devices to communicate in a wireless manner.	It refers to a network that connects two or more devices by using wireless data connections over short distances.
2.	The distance range is 30 feet to 100 feet.	The distance range is Up to 400 feet.
3.	It requires low bandwidth (not for transferring large files).	It requires high bandwidth.
4.	Bluetooth has generally lower speed.	Wireless LAN is much faster compared to Bluetooth.
5.	Lower cost.	Cost is much more expensive than Bluetooth.
6.	Bluetooth chips have lower power consumption - less drain on battery.	It requires more power consumption.
7.	It is less secure.	More secure.
8.	Fairly simple to use. Can be used to connect upto seven devices at a time. It is easy to switch between devices or find and connect to any device.	It is more complex and requires configuration of hardware and software.

PRACTICE QUESTIONS**Q. I Multiple Choice Questions:**

1. Which are the following lower layers of the OSI model?

(a) Physical layer	(b) Data link layer
(c) Both (a) and (b)	(d) None of these

2. Which layer is concerned with transmission of raw bits over a communication channel/medium?

(a) Physical layer	(b) Data link layer
(c) Network layer	(d) All of these
3. Which is responsible for the reliable transfer of data frames from one node to another connected by the physical layer?

(a) Physical layer	(b) Data link layer
(c) Network layer	(d) All of these
4. The two sublayers of the data link layer are _____.

(a) Logical Link Control (LLC)	(b) Medium Access Control (MAC)
(c) Both (a) and (b)	(d) None of these
5. The design issues of the data link layer are _____.

(a) Controlling over the flow of data	(b) Providing the service interface to the network layer
(c) Dealing with the transmission errors	(d) All of these
6. Breaking the bit stream into frames is called _____.

(a) Packetizing	(b) Framing
(c) Both (a) and (b)	(d) None of these
7. Which is a state occurring in the network layer when the message traffic is so heavy that it slows down network response time?

(a) Congestion	(b) Error
(c) Flow	(d) All of these
8. A link layer address is sometimes called as _____.

(a) a link address	(b) a physical address
(c) a MAC address	(d) All of these
9. Which method uses a field in the header to specify the number of characters in the frame?

(a) Character count	(b) Flag bytes with byte stuffing
(c) Starting and ending flags	(d) None of these
10. Which 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?

(a) LLC	(b) MAC
(c) Both (a) and (b)	(d) None of these

11. Which is a process in which a single channel is divided and allotted to multiple users in order to carry user specific tasks.
- (a) Data allocation
 - (b) Communication allocation
 - (c) Channel allocation
 - (d) All of these
12. In which channel allocation, frequency bands are not permanently assigned to the users?
- (a) Dynamic
 - (b) Static
 - (c) Fixed
 - (d) All of these
13. Which is a system for coordinating and arbitrating access to a shared communication Networks channel?
- (a) CSMA
 - (b) FDMA
 - (c) ALOHA
 - (d) None of these
14. Which is a network access method used on shared network topologies such as Ethernet to control access to the network?
- (a) CSMA
 - (b) FDMA
 - (c) ALOHA
 - (d) None of these
15. In which method, the station needs to make a "before sending data".
- (a) Polling
 - (b) Reservation
 - (c) Select
 - (d) None of these
16. Which is the multiple access method in which the available bandwidth of a link is shared in time, frequency or through code between different stations?
- (a) Polling
 - (b) Reservation
 - (c) Channelization
 - (d) None of these
17. Which is a channel access method for stored medium networks?
- (a) TDMA
 - (b) FDMA
 - (c) CDMA
 - (d) All of these
18. A switched network consists of a series of interlinked nodes called ____.
- (a) Switches
 - (b) Routers
 - (c) Repeaters
 - (d) All of these
19. Which switching takes place at the physical layer of the TCP/IP reference model?
- (a) Message
 - (b) Packet
 - (c) Circuit
 - (d) None of these
20. Virtual circuit packet switching is normally done at the _____ layer.
- (a) Physical
 - (b) Data link
 - (c) Network
 - (d) None of these

21. Which is a standardized system for connecting computers to a LAN?
- (a) Twisted pair
 - (b) Coaxial cable
 - (c) Ethernet
 - (d) None of these
22. Which standard defines rules for configuring an Ethernet network?
- (a) 802.3
 - (b) 802.3u
 - (c) 802.ba
 - (d) None of these
23. Which is a type of contention oriented protocol that defines how to respond when a collision is detected?
- (a) CSMA
 - (b) CSMA/CA
 - (c) CSMA/CD
 - (d) None of these
24. Which standard is defined for wireless LAN?
- (a) IEEE 802.3
 - (b) IEEE 802.11
 - (c) IEEE 802.ba
 - (d) IEEE 802.3u
25. A _____ with an AP is called an infrastructure network.
- (a) BSS
 - (b) DS
 - (c) ESS
 - (d) None of these
26. Which is a short-range (below 30 ft.) wireless radio technology that allows electronic devices to connect to one another?
- (a) WiMax
 - (b) Bluetooth
 - (c) WiFi
 - (d) None of these

ANSWERS

1. (c)	2. (a)	3. (b)	4. (c)	5. (d)	6. (b)	7. (a)
8. (d)	9. (a)	10.(b)	11. (c)	12. (a)	13. (c)	14. (a)
15. (b)	16. (c)	17. (a)	18. (a)	19. (c)	20. (b)	21. (c)
22. (a)	23. (c)	24. (b)	25. (a)	26. (b)		

Q. II Fill in the Blanks:

1. The _____ layer provides services to data link layer.
2. The _____ provides for the transfer of data frames between hosts connected to the physical link.
3. Signals can be either _____ or _____.
4. Digital data refers to information that has _____ states.
5. The maximum rate at which data can be correctly communicated over a channel in presence of noise and distortion is known as its _____ capacity.

6. The term _____ refers to the speed of data transmissions.
7. _____ is the rate of successful message delivery over a communication channel/medium.
8. _____ is the time it takes for a packet to get across the network, from source to destination.
9. The _____ product defines the number of bits that can fill the network link.
10. _____ is the variance in time delay in milliseconds (ms) between data packets over a network. It is a disruption in the normal sequence of sending data packets.
11. The _____ layer is located between the physical and the network layers.
12. _____ control design issue deals with transmission errors.
13. In _____ connectionless service, the sender machine sends the frames to the destination machine without having the destination machine acknowledge them.
14. Group of physical layer bits, stream into units (messages) called as _____.
15. _____ in the data link layer separates a message from one source to a destination by adding a sender address and a destination address.
16. _____ allocation may be done using two ways Static Channel Allocation and Dynamic Channel Allocation.
17. The traditional way of allocation the single channel for _____ users is the Frequency Division Multiplexing (FDM).
18. Media access methods are implemented at the _____ layer.
19. _____ was designed for a wireless LAN, but it can be used on any shared medium.
20. A station is allowed to send data when the station receives a special frame called _____.
21. In _____, the stations are organized in a logical ring.
22. In _____, the entire bandwidth is one channel.
23. At the _____ layer of the TCP/IP protocol suite, we can have only circuit switching.
24. At the data link layer of the TCP/IP protocol suite, we can have _____ switching.
25. In packet switching, each packet has _____ and destination addresses, travelling from one point (router) to the other point (router).
26. In packet switching, _____ are divided into packets of fixed or variable size.
27. A _____ is simply a collection of two or more computers, printers, and other devices linked by Ethernet cables.
28. Ethernet provides a _____ service which means each frame sent is independent of the previous or next frame.

29. _____ Ethernet is an Ethernet standard for 100-Mbps data transmission defined by the IEEE 802.3u specification.
30. The IEEE initial standard for _____ Ethernet was produced by the IEEE in June 1998 as IEEE 802.3z.
31. Wireless LANs are those Local Area Networks that use high frequency _____ waves instead of cables for connecting the devices in LAN.
32. A wired _____ LAN is a set of hosts connected via a link-layer switch.
33. An _____ is made up of two or more BSSs with APs.
34. A Bluetooth LAN is an _____ network.
35. _____ is formed by combining various piconets.
36. In the data link layer, _____ control restricts the number of frames the sender can send before it waits for an acknowledgment from the receiver.
37. _____ count method uses a field in the header to specify the number of characters in the frame.
38. _____ method allows data frames to contain an arbitrary number of bits and allows character codes with an arbitrary number of bits per character.
39. _____ channel allocation are schemes for allotting shared network channels to competing users in a dynamic manner as per their requirements.
40. The Bluetooth _____ layer performs functions similar to those in the Internet model's MAC sublayer.

ANSWERS

1. Physical	2. Data link	3. Analog, digital	4. Discredit
5. Channel	6. Bandwidth	7. Throughput	8. Latency
9. Bandwidth-delay	10. Jitter	11. Data link	12. Error
13. Unacknowledged	14. Frames	15. Framing	16. Channel
17. Multiple	18. Data link	19. Aloha	20. Token
21. Token passing	22. TDMA	23. Physical	24. Packet
25. Source	26. Messages	27. Wired network (LAN)	28. Connectionless
29. Fast	30. Gigabit	31. Radio	32. Isolated
33. ESS	34. Ad hoc	35. Scattemet	36. Flow
37. Character	38. Bit stuffing	39. Dynamic	40. Baseband

Q. III State True or False:

1. The physical layer (layer 1) of OSI and TCP/IP models deals with transmission of individual bits from one node to another over a physical medium.
2. Digital signals have infinite values in a range and Digital Signals have a limited number of defined values.
3. Digital data takes on discrete values. For example, data is stored in computer memory in the form of 0s and 1s.
4. Propagation time measures the time required for a bit to travel from the source to destination.
5. The data link layer is layer number 2 in the ISO-OSI and TCP/IP model.
6. Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
7. The data link layer divides the stream of bits received from the network layer into manageable data units called packets.
8. The data link layer ensures error free link for data transmission.
9. A link is controlled at the data link layer, the addresses need to belong to the data link layer.
10. In static channel allocation, a fixed portion of the frequency channel is allotted to each competing user.
11. CSMA/CD stands for Carrier Sense Multiple Access with Collision Detection.
12. CSMA/CA stands for Carrier Sense Multipoint Access with Collision Avoidance.
13. In FDMA (Frequency Division Multiple Access), the bandwidth is shared by all stations.
14. In CDMA (Code Division Multiple Access), only one channel occupies the entire bandwidth of the link. All stations can send data simultaneously.
15. FDMA is an access method in the physical layer.
16. In packet switching, each packet has source and destination addresses, travelling from one point (router) to the other point (router).
17. In Virtual Circuit Packet Switching, packets are sent in sequential order over a defined route.
18. In message switching, it is not necessary to establish a dedicated path between transmitter and receiver.
19. The IEEE has subdivided the data link layer into two sub layers i.e. LLC (Logical Link Control) and MAC (Media Access Control).

20. A wireless isolated LAN, called an ad hoc network in wireless LAN terminology, is a set of hosts that communicate freely with each other.
21. A ESS is made up of stationary or mobile wireless station and an optional central base station, known as Access Point (AP).
22. IEEE 802.11 defines two MAC sublayers, Distribution Co-ordination Function (DCF) and Point Co-ordination Function (PCF).
23. The Point Co-ordination Function (PCF) is an optional access method which is implemented in an infrastructure network and not in ad hoc network.
24. Piconet is a Bluetooth network that consists of one primary (master) node and seven active secondary (slave) nodes.
25. Bandwidth describes the volume of data that can be transferred at a given time.
26. Throughput is the actual amount of data that is successfully sent/received over the communication link.
27. Jitter variation in packet delay at the receiver of the information.
28. Throughput refers to measurement of data transferred in a specific time period.
29. Flow control in the data link layer is the process of detecting and correcting data frames that have been corrupted or lost during transmission.
30. In the dynamic channel allocation scheme, a fixed portion of the frequency channel is allotted to each user.
31. In 1-persistent CSMA method, a station that wants to transmit data continuously senses the channel to check whether the channel is idle or busy.
32. In controlled access, the stations consult one another to find which station has the right to send.
33. Packet switching is a method of transferring the data to a network in form of packets.
34. A Gigabit Ethernet network can transmit data at a rate up to 10 Megabits per second (10 Mbps).
35. The Fast Ethernet standard (IEEE 802.3u) has been established for Ethernet networks that need higher transmission speeds. This standard raises the Ethernet speed limit from 10 Mbps to 100 Mbps.
36. There are three types of Fast Ethernet: 100BASE-TX for use with level 5 UTP cable; 100BASE-FX for use with fiber-optic cable; and 100BASE-T4 which utilizes an extra two wires for use with level 3 UTP cable. The 100BASE-TX standard has become the most popular due to its close compatibility with the 10BASE-T Ethernet standard.

37. Gigabit Ethernet (GbE) is the family of Ethernet technologies that achieve theoretical data rates of 1 gigabit per second (1 Gbps).
38. Wired LANs are wireless computer networks that use high-frequency radio waves instead of cables for connecting the devices within a limited area forming LAN.
39. The IEEE 802.11 standard for wireless LANs defines two services: basic service set (BSS) and extended service set (ESS).
40. The physical layer methods used by wireless LANs include frequency-hopping spread spectrum (FHSS), direct sequence spread spectrum (DSSS), orthogonal frequency-division multiplexing (OFDM), and high-rate direct sequence spread spectrum (HR-DSSS).
41. The network allocation vector (NAV) is a timer used for collision avoidance.
42. The Bluetooth radio layer performs functions similar to those in the Internet model's physical layer.

ANSWERS

1. (T)	2. (F)	3. (T)	4. (T)	5. (T)	6. (T)
7. (F)	8. (T)	9. (T)	10. (T)	11. (F)	12. (F)
13. (F)	14. (T)	15. (F)	16. (T)	17. (T)	18. (T)
19. (T)	20. (T)	21. (F)	22. (T)	23. (T)	24. (F)
25. (T)	26. (T)	27. (T)	28. (T)	29. (F)	30. (F)
31. (T)	32. (T)	33. (T)	34. (F)	45. (T)	36. (T)
37. (T)	38. (F)	39. (T)	40. (T)	41. (T)	42. (T)

Q. IV Answer the following Questions:

(A) Short Answer Questions:

1. List lower layers in OSI model.
2. What is bandwidth?
3. Define the term latency (delay).
4. What is throughput?
5. Define the term framing?
6. What is jitter?
7. List design issues of data link layer.
8. What is a frame?
9. List services of data link layer.
10. What is flow control?

11. Define congestion?
12. List various framing methods.
13. What is meant by channel allocation?
14. What is ALOHA?
15. What is CSMA?
16. What is CSMA/CA?
17. What is CSMA/CD?
18. Define polling.
19. What is meant by channelization?
20. What is TDMA and FDMA?
21. Define switching.
22. List types of switching.
23. Give approaches for packet switching.
24. Define the term wired LANs.
25. What is Ethernet?
26. What is wireless LAN?
27. List components for IEEE 802.11 architecture.
28. What is Bluetooth?
29. List components for Bluetooth architecture.

(B) Long Answer Questions:

1. With the help of diagrams describe communication at the physical layer.
 2. Write Nyquist and Shannon's formula for calculating data rate of a channel.
 3. Define framing? Explain frame format with its different fields.
 4. Describe error control in detail.
 5. Explain the term congestion control in detail.
 6. Write short note on: Link layer addressing.
 7. With a suitable diagram describe the character count method.
 8. Describe the term flag bytes with byte stuffing.
 9. Explain physical layer coding violations in detail.
 10. What is static and dynamic channel allocation? Compare them.
 11. Explain slotted and pure ALOHA.
 12. Compare CSMA/CA and CSMA/CD.
 13. Describe access control diagrammatically.
-

14. Explain the term token passing in detail.
15. Define channelization. Also explain FDMA and TDMA.
16. Explain packet switching diagrammatically.
17. What is circuit switching? How does it work? State its advantages and disadvantages.
18. With the help of diagram describe message switching.
19. Differentiate between circuit, packet and message switching.
20. With the help of example describe datagram packet switching.
21. With the help of example, describe virtual circuit packet switching.
22. Explain wired and wireless LANs. Also compare them.
23. Explain following Ethernet with implementations:
 - (i) Fast Ethernet
 - (ii) Gigabit Ethernet.
24. Explain isolated LANs diagrammatically.
25. Describe IEEE 802.11 architecture in detail.
26. What are the responsibilities of a MAC sublayer? Also explain its frame format.
27. With the help of diagrams describe Bluetooth architecture.
28. List advantages, disadvantages and applications of Bluetooth.

UNIVERSITY QUESTIONS AND ANSWERS

April 2016

1. Apply bit stuffing on the pattern: 0100111111101111110. **[1 M]**
- Ans.** Refer to Section 2.3.3.
2. List any two channelization protocols. **[1 M]**
- Ans.** Refer to Section 2.4.5.
3. Explain Pure ALOHA and slotted ALOHA with example. **[5 M]**
- Ans.** Refer to Section 2.4.3.1 Point (1).
4. Explain circuit switching in detail. **[5 M]**
- Ans.** Refer to Section 2.5.1.1.
5. Explain Polling "Select" function. **[3 M]**
- Ans.** Refer to Section 2.4.4.
6. Which types of services are defined by IEEE 802.11? **[1 M]**
- Ans.** Refer to Section 2.7.4.

7. What is Ethernet? Give its type with a short description.

[5 M]

Ans. Refer to Section 2.6.1.

8. Give any four goals of Fast Ethernet.

[2 M]

Ans. Refer to Section 2.6.5.

April 2017

1. What is framing? Explain any two framing methods with examples.

[4 M]

Ans. Refer to Sections 2.2.3 and 2.3.

2. Explain FDMA in detail.

[4 M]

Ans. Refer to Section 2.4.5 Point (1).

3. What are Random access methods? Explain any one mechanism.

[4 M]

Ans. Refer to Section 2.4.3.1.

4. Explain Polling "Select" function.

[3 M]

Ans. Refer to Section 2.4.4.

5. Which standard is used for wireless LAN?

[1 M]

Ans. Refer to Section 2.7.

6. What is Bluetooth? Write any two advantages of Bluetooth.

[2 M]

Ans. Refer to Sections 2.7.7 and 2.7.7.4.

October 2017

1. State the strategies used to avoid collisions.

[1 M]

Ans. Refer to Section 2.4.3.1.

2. Explain the packet switching with advantages and disadvantages.

[5 M]

Ans. Refer to Section 2.5.1.2.

3. Describe the functions performed by Data Link Layer.

[5 M]

Ans. Refer to Sections 2.0 and 2.2.

4. Consider a CDMA scheme with 3 stations having chip sequences $[+1 -1 +1 -1]$, $[+1 +1 -1 -1]$. Station 1 sends bit 1. Station 2 sends bit 0. Station 3 is silent.

Show the process of encoding and decoding along with the signals.

[5 M]

Ans. Refer to Section 2.4.3.1, Point (2).

5. Describe Pure and Slotted ALOHA in brief.

[5 M]

Ans. Refer to Section 2.4.3.1, Point (1).

6. Why is CSMA/CD not required in full duplex switched Ethernet?

[1 M]

Ans. Refer to Section 2.6.3.

7. State any two applications of wireless LAN.	[1 M]
Ans. Refer to Section 2.7.	
8. Explain in detail 802.3 MAC frame format.	[3 M]
Ans. Refer to Section 2.7.6.1.	
9. Write any two applications of Bluetooth technology.	[2 M]
Ans. Refer to Section 2.7.7.4.	

April 2018

1. What is the responsibility of a Physical Layer.	[1 M]
Ans. Refer to Section 2.7.5.	
2. List the cables used with Ethernet LAN.	[1 M]
Ans. Refer to Section 2.6.1.	
3. A telephone network is an example of a circuit switched network. State True/False.	[1 M]
Ans. Refer to Section 2.5.1.1.	
4. Consider a CDMA scheme with 3 stations having chip sequences $[+1 -1 +1 -1]$, $[+1 +1 -1 -1]$ and $[1+ +1 +1 +1]$. Station 1 sends bit 1. Station 2 sends bit 0. Station 3 is silent. Show the process of encoding and decoding along with the signals.	[5 M]
Ans. Refer to Section 2.4.3.1, Point (3).	
5. Explain the strategies used by CSMA/CA.	[4 M]
Ans. Refer to Section 2.4.3.1, Point (4).	
6. What is Framing? List methods of framing.	[2 M]
Ans. Refer to Sections 2.2.3 and 2.3.	
7. Compare the circuit and packet switching.	[4 M]
Ans. Refer to Page No 2.51.	
8. Draw BSS with an access point.	[1 M]
Ans. Refer to Section 2.7.4, Point (1).	
9. Draw the frame format of Ethernet.	[2 M]
Ans. Refer to Section 2.6.1.1, Point (3).	

October 2018

1. If the bandwidth of the channel is 10 kbps, how long does it take to transmit a frame of 100000 bits?	[1 M]
Ans. Refer to Section 2.1.1.	

2. What is flow control? Why is it needed?

[1 M]

Ans. Refer to Section 2.2.4.

3. Calculate the total delay for a frame of size 5 million bits which is sent on a link with 10 routers, each having queuing time $2 \mu\text{s}$ and a processing time of $1 \mu\text{s}$. The length of the link is 2000 km and speed of light is $2 \times 10^8 \text{ m/s}$ in the link. The link has bandwidth 5 mbps.

[5 M]

Ans. Refer to Section 2.1.1.

4. What is framing? Explain any two framing methods with examples.

[5 M]

Ans. Refer to Sections 2.2.3 and 2.3.

5. Write a note on the Reservation method used in controlled access.

[3 M]

Ans. Refer to Section 2.4.4, Point (1).

6. What is channelization? List three channelization methods and explain any one method.

[5 M]

Ans. Refer to Section 2.4.5.

7. State the minimum and maximum Ethernet frame length.

[1 M]

Ans. Refer to 2.6.1.1, Point (3).

8. How many maximum no of computers is used to create Piconet?

[1 M]

Ans. Refer to Section 2.7.7.1, Point (1).

9. Explain the types of traditional Ethernet.

[5 M]

Ans. Refer to Section 2.6.1.

10. Explain Polling "Select" function.

[3 M]

Ans. Refer to Section 2.4.4.

11. Explain the datagram circuit and virtual circuit in detail.

[4 M]

Ans. Refer to Section 2.5.1.2.

12. Explain BSS and its types with diagrams.

[4 M]

Ans. Refer to Section 2.7.4, Point (1).

April 2019

1. If a composite signal is composed of five sine waves of frequencies 100, 300, 500, 700 and 900 Hz. What is the bandwidth of the signal?

[1 M]

Ans. Refer to Section 2.1.1.

2. Calculate maximum bit rate using Shannon's theorem for a channel having bandwidth 31000 Hz and S/N ratio 20dB.

[5 M]

Ans. Refer to Section 2.1.1.

3. Explain the data link protocols for noiseless channels.

[5 M]

Ans. Refer to Section 2.1.1.

4. State the difference between reservation and polling.

[3 M]

Ans. Refer to Section 2.4.4 Points (1) and (2).

5. What is channelization? List the methods of channelization. Explain any one method.

[5 M]

Ans. Refer to Section 2.4.5.

6. Give difference between WLAN and Bluetooth.

[5 M]

Ans. Refer to Page No. 2.84.

7. Explain 10Base5, 10Base2, 10Base-T, 10Base-F.

[4 M]

Ans. Refer to Section 2.6.4.



Network Layer

Objectives...

- To understand Network Layer
- To study IPv4 and Addressing
- To learn Basic Concepts in IPv6
- To understand Congestion Control
- To learn Mobile IP and Routing

3.0

INTRODUCTION

(April 16)

- Network layer is responsible for host-to-host delivery of the messages (datagrams) between two hosts.
- The network layer controls the source to destination delivery of data packets across multiple hops (nodes).
- Network layer is responsible for routing packets from the source host to the destination host. Network layer also provides mechanisms for congestion control.
- Network layer is also responsible for fragmentation in which large size packets are broken down into smaller packets/fragments.

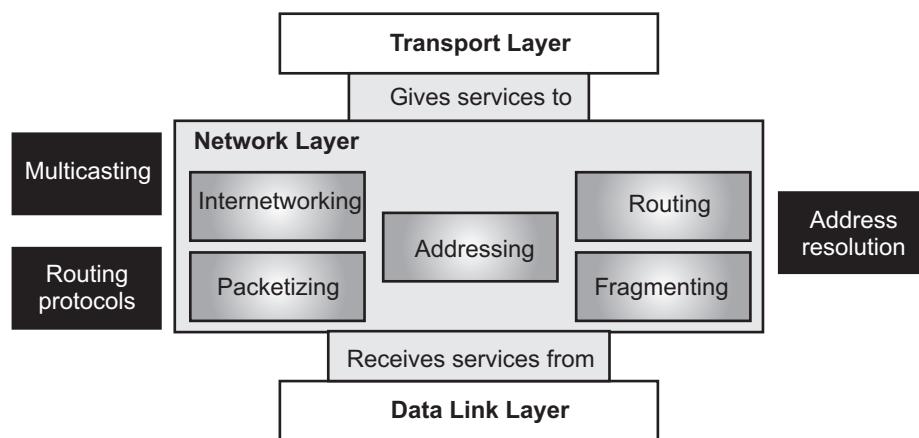


Fig. 3.1: Position of Network Layer

- When the data packets are routed to remote locations, a logical addressing scheme is required to differentiate between the source system and the destination system. This is provided by the network layer.
- One of the main functions of network layer is to provide internetworking between different networks. It provides a logical connection between different types of network.
- Fig. 3.1 shows position of network layer in OSI Model.

3.1 NETWORK LAYER SERVICES

(Oct. 18)

- The services which are offered by the network layer are as follows:

1. Packetizing:

- The process of encapsulating the data received from upper layers of the network (also called as payload) in a network layer packet at the source and decapsulating the payload from the network layer packet at the destination is known as packetizing.
- In other words, one responsibility of the network layer is to carry the data packets from the source to the destination without changing it or using it.
- The network layer is doing the service of a carrier such as the postal office, is responsible for delivery of packages from sender to a receiver without changing or using the content.
- The source host adds a header that contains the source and destination address and some other relevant information required by the network layer protocol to the payload received from the upper layer protocol, and delivers the packet to the data link layer.
- The destination host receives the network layer packet from its data link layer, decapsulates the packet, and delivers the payload to the corresponding upper layer protocol.
- The routers in the path are not allowed to change either the source or the destination address.
- The routers in the path are not allowed to decapsulate the packets they receive unless they need to be fragmented.
- Packetizing is done by Internet Protocol (IP) that defines its own packet format.

2. Routing and Forwarding:

- Routing and forwarding are two other services offered by the network layer.
- The network layer is responsible for routing the packets from its source to the destination. With the help of forwarding, data packets are transferred from one place to another in the network.

- In a network, there are a number of routes available from the source to the destination. The network layer has some strategies which find out the best possible route. This process is referred to as routing.
- There are a number of routing protocols which are used in the routing process and they should be run to help the routers coordinate with each other and help in establishing communication throughout the network.
- Forwarding is simply defined as the action applied by each router when a packet arrives at one of its interfaces.
- Normally, a router uses the decision making table for applying this action sometimes called the forwarding table and sometimes the routing table.
- When a router receives a packet from one of its attached networks, it needs to forward the packet to another attached network (unicast routing) or to some attached networks (in case of multicast routing).

Other Services:**1. Flow Control:**

- It regulates the amount of data a source can send without overloading the receiver.
- If the source produces data at a very faster rate than the receiver can consume it, the receiver will be overloaded with data.
- To control the flow of data, the receiver should send feedback to the sender to inform the latter that it is overloaded with data.
- There is a lack of flow control in the design of the network layer. It does not directly provide any flow control.
- The datagrams are sent by the sender when they are ready, without any attention to the readiness of the receiver.

2. Error Control:

- Error control also in the network layer is the process of detecting and correcting data packets that have been corrupted or lost during transmission.
- For error control network layer uses ICMP protocol. Internet Control Message Protocol (ICMP) is a network layer protocol that reports errors and provides information related to IP packet processing.
- ICMP is used by network devices to send error messages indicating, for example, that a requested service is not available or that a host is not reachable.

3. Quality of Service:

- The Internet has thrived by providing better quality of service to support applications like real-time communication of audio and video.

4. Congestion Control:

- Congestion is a situation in a network layer in which too many datagrams are present in an area of the Internet.
- Congestion occurs when the number of datagrams sent by source is beyond the capacity of network or routers.
- If congestion continues, sometimes a situation may arrive where the system collapses and no datagrams are delivered.
- Although congestion control is indirectly implemented in the network layer, there is still a lack of congestion control in the network layer.

5. Security:

- The network layer was designed with no security provision. The network layer uses a virtual level IPSec for security.

3.2 CONGESTION CONTROL (OPEN AND CLOSED LOOP)

- Congestion control refers to the techniques used to control or prevent congestion.

Basic Concept of Congestion:

(Oct. 18, April 19)

- Congestion in a network may occur if the load on the network (the number of packets sent to the network) is greater than the capacity of the network (the number of packets a network can handle).
- Congestion control refers to the mechanisms and techniques to control the congestion and keep the load on the network below the capacity.

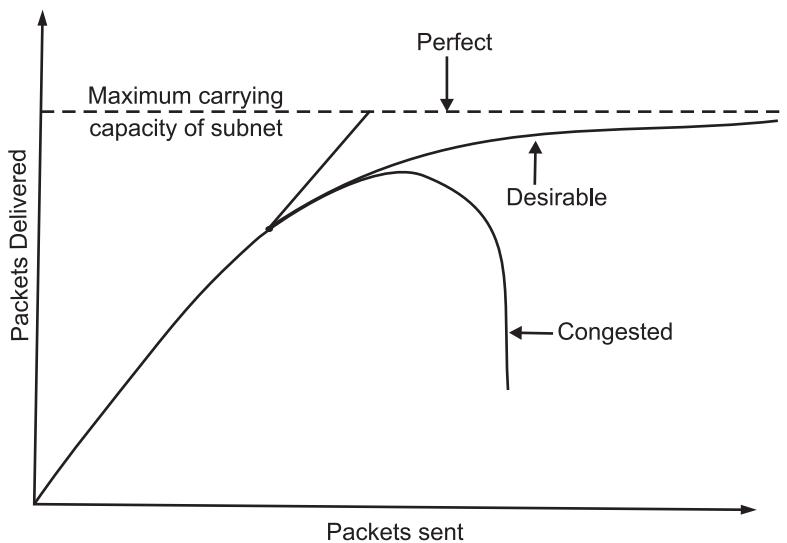


Fig. 3.2: When too Many Packets are Sent, Congestion Occurs and Performance Degrades

- At very high traffic, performance collapses completely and almost no packets are delivered. Buffers get full, so packets are discarded leading to more retransmissions and less packets delivered to their destinations.
- Congestion thus tends to feed upon itself and become worse, leading to collapse of the system.
- Congestion can occur because of several reasons:
 1. If there is insufficient memory at the router to hold the packets, congestion occurs and packets are lost.
 2. Slow processors can also cause congestion. If the router's processor is slow, queues can build up, even though there is excess line capacity, congestion can occur.
 3. Similarly, low bandwidth lines can also cause congestion.

Basic Concept of Congestion Control:

- Congestion control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened.
- Congestion control mechanisms are divided into two categories, one category prevents the congestion from happening (open loop congestion control) and the other category removes (closed loop congestion control) congestion after it has taken place.

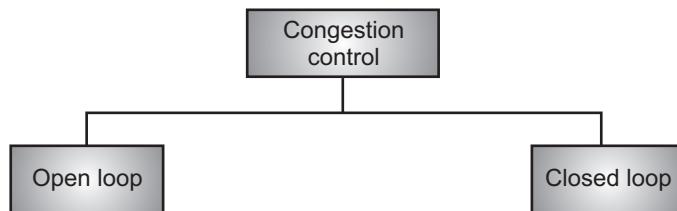


Fig. 3.3: Mechanisms for Congestion Control

1. Open Loop Congestion Control:

(Oct. 17)

- Open loop congestion control policies are applied to prevent congestion before it happens.
- The congestion control is handled either by the source or the destination.
- Policies adopted by open loop congestion control are explained below:
 - (i) **Retransmission Policy:** It is the policy in which retransmission of the packets are taken care. If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted. This transmission may increase the congestion in the network. To prevent congestion, retransmission timers must be designed to prevent congestion and also able to optimize efficiency.
 - (ii) **Window Policy:** The type of window at the sender side may also affect the congestion. Several packets in the Go-Back-N window are present, although some

packets may be received successfully at the receiver side. This duplication may increase the congestion in the network and make it worse. Therefore, a Selective repeat window should be adopted as it sends the specific packet that may have been lost.

- (iii) **Discarding Policy:** A good discarding policy adopted by the routers is that the routers may prevent congestion and at the same time partially discards the corrupted or less sensitive package and also be able to maintain the quality of a message. In case of audio file transmission, routers can discard less sensitive packets to prevent congestion and also maintain the quality of the audio file.
 - (iv) **Acknowledgment Policy:** Since acknowledgement is also part of the load in the network, the acknowledgement policy imposed by the receiver may also affect congestion. Several approaches can be used to prevent congestion related to acknowledgment. The receiver should send acknowledgement for N packets rather than sending acknowledgement for a single packet. The receiver should send an acknowledgment only if it has to send a packet or a timer expires.
 - (v) **Admission Policy:** In admission policy a mechanism should be used to prevent congestion. Switches in a flow should first check the resource requirement of a network flow before transmitting it further. If there is a chance of a congestion or there is a congestion in the network, the router should deny establishing a virtual network connection to prevent further congestion.
 - All the above policies are adopted to prevent congestion before it happens in the network.
- 2. Closed Loop Congestion Control:** (Oct. 17)
- Closed loop congestion control technique is used to treat or alleviate congestion after it happens. Closed loop solutions are based on feedback loops.
 - Closed loop congestion control has following three parts:
 - (i) Monitor the system to detect when and where congestion occurs.
 - (ii) Pass this information to places where action can be taken.
 - (iii) Adjust system operations to correct the problem.
 - Policies adopted by open loop congestion control are explained below:
 - (i) **Backpressure:** Backpressure is a technique in which a congested node stops receiving packets from upstream nodes. This may cause the upstream node or nodes to become congested and rejects receiving data from above nodes. Backpressure is a node-to-node congestion control technique that propagates in the opposite direction of data flow. The backpressure technique can be applied

only to virtual circuits where each node has information of its above upstream node.

In the Fig. 3.4, the 3rd node is congested and stops receiving packets as a result 2nd node may get congested due to slowing down of the output data flow. Similarly, 1st node may get congested and inform the source to slow down.

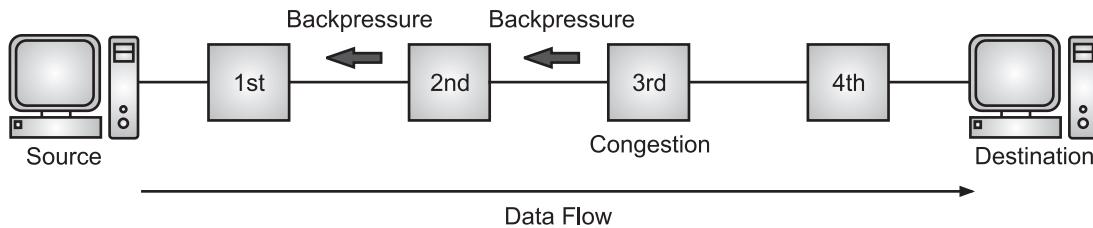


Fig. 3.4

- (ii) **Choke Packet Technique:** Choke packet technique is applicable to both virtual networks as well as datagram subnets. A choke packet is a packet sent by a node to the source to inform it of congestion. Each router monitors its resources and the utilization at each of its output lines. whenever the resource utilization exceeds the threshold value which is set by the administrator, the router directly sends a choke packet to the source giving it a feedback to reduce the traffic. The intermediate nodes through which the packets have traveled are not warned about congestion. Fig. 3.5 shows the idea of a choke packet.

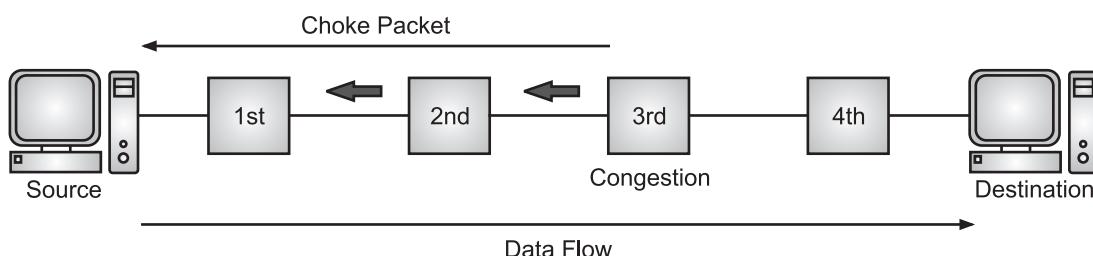


Fig. 3.5

- (iii) **Implicit Signaling:** In implicit signaling, there is no communication between the congested nodes and the source. The source guesses that there is congestion in a network. For example, the when the sender sends several packets and there is no acknowledgement for a while, one assumption is that there is a congestion.

- (iv) **Explicit Signaling:** In explicit signaling, if a node experiences congestion it can explicitly send a packet to the source or destination to inform about congestion. The difference between choke packet and explicit signaling is that the signal is included in the packets that carry data rather than creating different packets as in case of choke packet technique. Explicit signaling can occur in either forward or backward direction.

- **Forward Signaling:** In forward signaling a signal is sent in the direction of the congestion. The destination is warned about congestion. The receiver in this case adopts policies to prevent further congestion.
- **Backward Signaling:** In backward signaling a signal is sent in the opposite direction of the congestion. The source is warned about congestion and it needs to slow down.

3.3 IPv4 ADDRESSING

- The Internet Protocol version 4 (IPv4), is responsible for packetizing, forwarding and delivery of a packet at the network layer.
- Internet Protocol (IP) is a set of rules that dictate how data should be delivered over the Internet.
- Networks using the TCP/IP protocol route messages based on the IP address of the destination.
- IP addressing is the method used to identify hosts and network devices in a network.
- The Internet Protocol Address (IP Address) is a unique number assigned to every computing device, such as personal computers, tablets, and smartphones used to identify itself and communicate with other devices in the IP network. Any device connected to the IP network must have a unique IP address within the network.
- Following are the two versions of the Internet Protocol (IP) are in common uses in the Internet today:
 1. An **Internet Protocol version 4 (IPv4) address** is a 32-bits address that uniquely and universally defines the connection of a host or a router to the Internet.
 2. The growth of the Internet and the depletion of available IPv4 addresses, a new version of IP, **Internet Protocol version 6 (IPv6)**, using 128-bits for the IP address, was developed in 1995.
- In this section, we study IP addressing in detail with IPv4 addressing. 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.

Basic Concept of IP Address/IPv4 Address:

(April 16, 17, 18, 19; Oct. 17)

- An IP address is an address used to uniquely identify a device on an IP network. The identifier used in the TCP/IP protocol suite to identify the connection of each device to the Internet called as the Internet Protocol address (IP address).
- An IP address is a numerical (32-bits) representation that uniquely identifies a specific interface on the network.
- 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.

- 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. Fig. 3.6 shows an IP address format.
- An IP address consists of two parts namely, a **Network ID**, which specifies the network on which a host resides, and a **Host ID**, which identifies the host within that network.

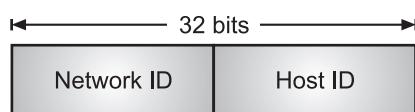


Fig. 3.6: Parts/Format of an IP Address

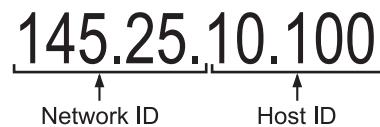


Fig. 3.7: Example of an IP Address

3.3.1 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-bits 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.
- There are three common notations to show an IPv4 address namely, binary notation (base 2), dotted-decimal notation (base 256), and hexadecimal notation (base 16).
- Fig. 3.8 shows all the three notations for IPv4 address.
- The notations for IP address are explained below:

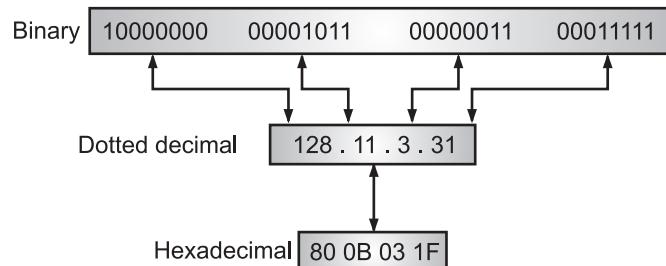


Fig. 3.8: Three Notations of IPv4 Addressing

1. **Binary Notation (Base 2):** Binary notation is the format that systems on the network use to process the address. In binary notation the IPv4 address is displayed as 32 bits. Each octet is often referred to as a byte. So it is common to hear an IPv4 address referred to as a 32-bit address or a 4-byte address. An example of binary notation is 01110101.10010101.00011101.11101010.
2. **Hexadecimal Notation (Base 16):** We sometimes see an IPv4 address in hexadecimal notation. Each hexadecimal digit is equivalent to four bits. This means that a 32-bits address has 8 hexadecimal digits. This notation is often used in network programming. An example of hexadecimal notation of an IPv4 address is C0.A8.01.64.

3. Dotted-decimal Notation (Base 256): To make the IPv4 address more compact and easier to read, Internet addresses are usually written in decimal form with a decimal point (dot) separating the bytes. Dotted-decimal notation is the format that is typically used for displaying the IP address in a human-readable format. An example of dotted-decimal notation is 192.168.1.100.

Examples:

Example 1: Change the following IPv4 addresses from binary notation to dotted-decimal notation.

- (i) 10000001 00001011 00001011 11101111
- (ii) 11000001 10000011 00011011 11111111
- (iii) 11100111 11011011 10001011 01101111
- (iv) 11111001 10011011 11111011 00001111

Solution:

We replace each group of 8 bits with its equivalent decimal number and add dots for separation.

- (i) 129.11.11.239
 - (ii) 193.131.27.255
 - (iii) 231.219.139.111
 - (iv) 249.155.251.15
-

Example 2: Change the following IPv4 addresses from dotted-decimal notation to binary notation.

- (i) 111.56.45.78
- (ii) 221.34.7.82
- (iii) 241.8.56.12
- (iv) 75.45.34.78

Solution:

We replace each decimal number with its binary equivalent.

- (i) 01101111 00111000 00101101 01001110
 - (ii) 11011101 00100010 00000111 01010010
 - (iii) 11110001 00001000 00111000 00001100
 - (iv) 01001011 00101101 00100010 01001110
-

Example 3: Change the following IPv4 addresses from binary notation to hexadecimal notation.

- (i) 10000001 00001011 00001011 11101111
-

(ii) 11000001 10000011 00011011 11111111

Solution:

We replace each group of 4 bits with its hexadecimal equivalent. Note that hexadecimal notation normally has no added spaces or dots; however, 0X (or 0x) is added at the beginning or the subscript 16 at the end to show that the number is in hexadecimal.

(i) 0X810B0BEF or 810B0BEF16

(ii) 0XC1831BFF or C1831BFF16

Example 4: 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.

Example 5: Convert the following IPv4 addresses from decimal notation to binary notation if it is in correct form.

(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).

3.3.2 Classful Addressing

(April 16)

- Internet Protocol (IP) hierarchy contains several classes of IP Addresses to be used efficiently in various situations as per the requirement of hosts per network.
- IPv4 addressing uses the concept of classes. This architecture is called classful addressing.
- In classful addressing, the address space is divided into five classes namely A, B, C, D and E. Each class in classful addressing, occupies some part of the whole address space.

- In class A, the network length is 8 bits, but since the first bit, which is 0, defines the class, we can have only seven bits as the network identifier. This means there are only $2^7 = 128$ networks in the world that can have a class A address.
- In class B, the network length is 16 bits, but since the first two bits, which are $(10)_2$, define the class, we can have only 14 bits as the network identifier. This means there are only $2^{14} = 16384$ networks in the world that can have a class B address.
- All addresses that start with $(110)_2$, belong to class C. In class C, the network length is 24 bits, but since three bits define the class, we can have only 21 bits as the network identifier. This means there are $2^{21} = 2,097,152$ networks in the world that can have a class C address.
- Class D (1110_2) is not divided into NetworkID and HostID. It is used for multicast addresses. All addresses that start with 1111 in binary belong to class E. As in Class D, Class E is not divided into NetworkID and HostID and is used as reserve.

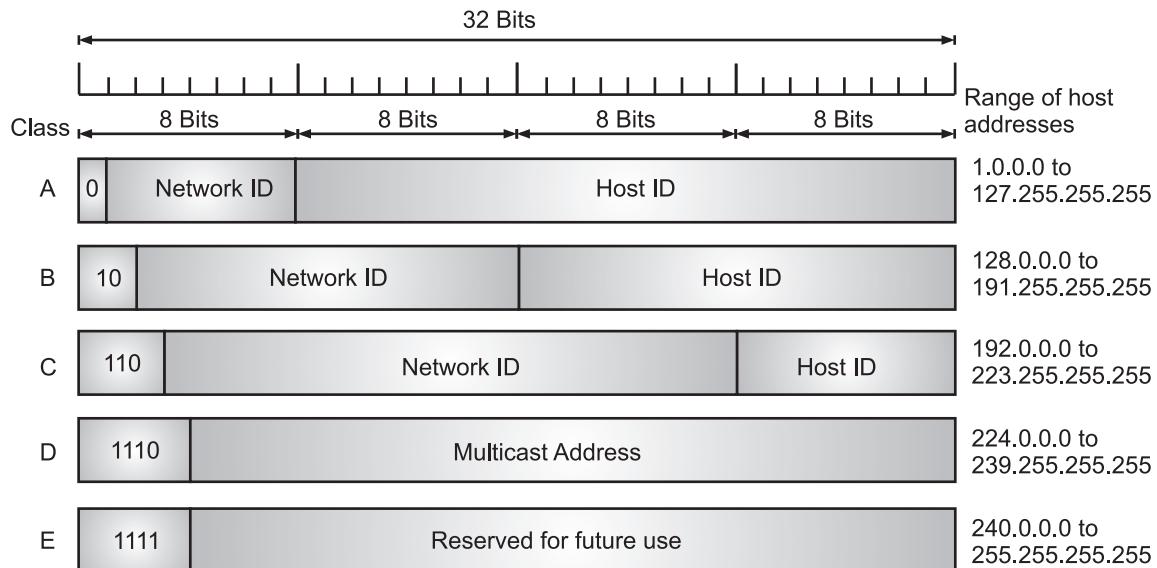


Fig. 3.9: Classful Addressing

Examples:**Example 1:** Find the class of each address:

- 00000001 00001011 00001011 11101111
- 11000001 10000011 00011011 11111111
- 10100111 11011011 10001011 01101111
- 11110011 10011011 11111011 00001111

Solution:

- The first bit is 0. This is a class A address.

-
- (ii) The first 2 bits are 1; the third bit is 0. This is a class C address.
 (iii) The first bit is 1; the second bit is 0. This is a class B address.
 (iv) The first 4 bits are 1s. This is a class E address.
-

Example 2: Find the class of each address:

- (i) 227.12.14.87
 (ii) 193.14.56.22
 (iii) 14.23.120.8
 (iv) 252.5.15.111

Solution:

- (i) The first byte is 227 (between 224 and 239); the class is D.
 (ii) The first byte is 193 (between 192 and 223); the class is C.
 (iii) The first byte is 14 (between 0 and 127); the class is A.
 (iv) The first byte is 252 (between 240 and 255); the class is E.
-

Basic Concept of Masking:

- A mask used to determine what subnet an IP address belongs to. A process that extracts the address of the physical network from an IP address is called Masking. If we do the subnetting, then masking extracts the subnetwork address from an IP address.
 - It may at first seem to be odd that IP address classes are assigned in this way. After all, there are not any private networks that have 16 million hosts on them, so it makes little sense even to have Class A addresses. However, it's possible to subdivide IP addresses even further by creating subnets on them.
 - A subnet is simply a subdivision of a network address that can be used to represent one LAN on an internetwork or the network of one of an ISP's clients.
 - Thus, a large ISP might have a Class A address registered to it and it might farm out pieces of the address to its clients in the form of subnets.
 - In many cases, a large ISP's clients are smaller ISPs, which in turn supply addresses to their own clients.
 - A subnet allows the flow of network traffic between hosts to be segregated based on a network configuration.
 - A subnet mask (or number) is used to determine the number of bits used for the subnet and host portions of the address.
 - The mask is a 32-bit value that uses one-bits for the network and subnet portions and zero-bits for the host portion.
-

Subnet Masks:

- IP networks can be divided into smaller networks called subnetworks (or 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.
- The network mask is used when a network is not subnetted.
- When we divide a network into several subnetworks, we need to create a subnetwork mask (or subnet mask) for each subnetwork.
- Fig. 3.10 shows a subnetwork has sub netid and hostid.
- Subnetting provides the following advantages:
 - Network Traffic Isolation:** There is less network traffic on each subnet.
 - Simplified Administration:** Networks may be managed independently.
 - Improved Security:** Subnets can isolate internal networks so they are not visible from external networks.
- A 14-bits subnet mask on a class B network only allows 2 node addresses for WAN links. A routing algorithm like OSPF (Open Shortest Path First) must be used for this approach.
- These protocols allow the Variable Length Subnet Masks (VLSM). RIP (Routing Information Protocol) and IGRP (Interior Gateway Routing Protocol) don't support this.
- Subnet mask information must be transmitted on the update packets for dynamic routing protocols for this to work.
- The router subnet mask is different from the WAN interface subnet mask. One network ID is required by each of:
 - Subnet,
 - WAN connection.
- One host ID is required by each of:
 - Each NIC on each host.
 - Each router interface.
- Types of subnet masks:
 - Default:** Fits into a Class A, B, or C network category.
 - Custom:** Used to break a default network such as a Class A, B or C network into subnets.

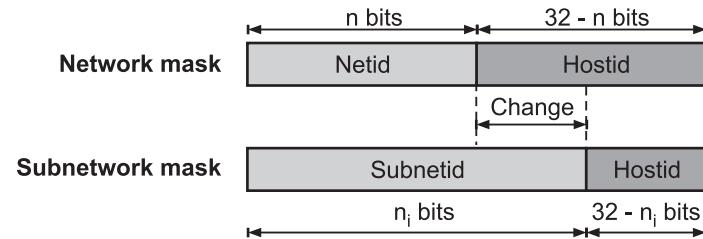


Fig. 3.10: Network Mask and Subnetwork Mask

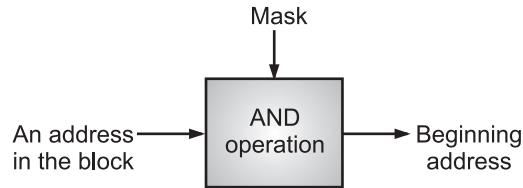


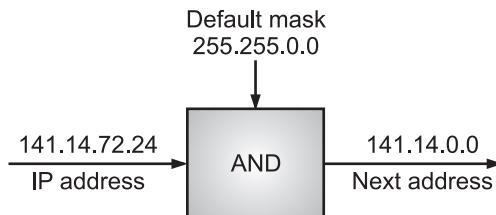
Fig. 3.11: Masking Concept



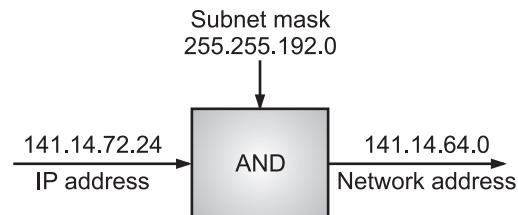
Fig. 3.12: AND Operation

Default Masks

Class	Mask in Binary	Mask in Dotted-decimal
A	11111111 00000000 00000000 00000000	255.0.0.0
B	11111111 11111111 00000000 00000000	255.255.0.0
C	11111111 11111111 11111111 00000000	255.255.255.0



(a) Without Subnetting



(b) With Subnetting

Fig. 3.13: Default Mask and Subnet Mask

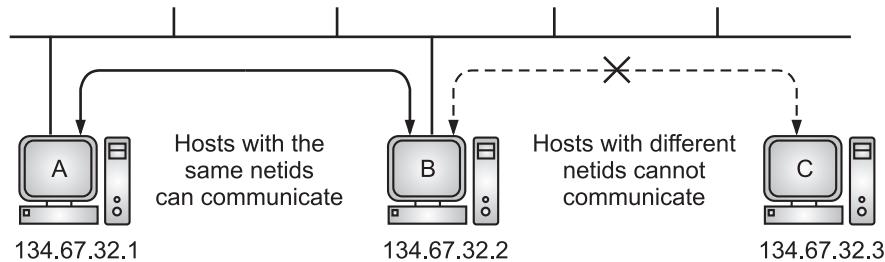


Fig. 3.14: Host Communication on a Local Network

- A subnet is defined by applying a bitmask, the subnet mask, to the IP address. If a bit is on the mask, the equivalent bit in the address is interpreted as a network bit.

- If the bit in the mask is off, the bit belongs to the host part of the address. The subnet is only known locally. To the rest of the Internet, the address is still interpreted as a standard IP address.

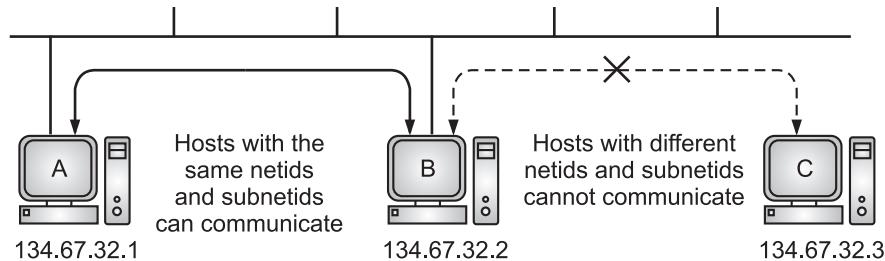


Fig. 3.15: Host Communication with Subnetting

Examples: Find the subnetwork address for the following.

Sr. No.	IP Address	Mask
1.	141.181.14.16	255.255.225.0
2.	200.34.22.156	255.255.255.240
3.	125.35.12.57	255.255.0.0

Solution:

1.	141.181.14.16	IP Address
	255.255.224.0	Mask
	141.181.0.0	Subnetwork Address
2.	200.34.22.156	IP Address
	255.255.255.240	Mask
	200.34.22.144	Subnetwork Address
3.	125.35.12.57	IP Address
	255.255.0.0	Mask
	125.35.0.0	Subnetwork Address

3.3.3 Subnetting

(April 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 defined as, “the process of dividing (partitioning) a network into several smaller networks (subnets)”.
- Subnetting is a method for partitioning/dividing a classful IP network into smaller subnetworks (subnets).

- The process of subnetting involves dividing a network up into smaller networks called subnets or sub networks.
- A subnet is a logical partition of an IP network into multiple, smaller network segments. Each of these subnets has its own specific address.
- To create these additional sub networks, we use a subnet mask. The subnet mask simply determines which portion of the IP address belongs to the host.
- The subnet address is created by dividing the host address into network address and host address.
- To subnet a network, extend the natural mask using some of the bits from the host ID portion of the address to create a subnetwork ID.
- For example, given a Class C network of 204.15.5.0 which has a natural mask of 255.255.255.0. We can create subnets in the following manner:

204.15.5.0	11001100.00001111.00000101.00000000
255.255.255.224	11111111.11111111.11111111.11100000
----- (sub)-----	

- By extending the mask to be 255.255.255.224, we have taken three bits (seen above as "sub") from the original host portion of the address and used them to make subnets. With these three bits, it is possible to create eight subnets.
- With the remaining five host ID bits. Each subnet can have up to 32 host addresses, 30 of which can actually be assigned to a device since host ids of zeros or all ones are not allowed (it is very important to remember this).
- So, with this in mind, the following subnets have been created:

204.15.5.0	255.255.255.224	host address range 1 to 30
204.15.5.32	255.255.255.224	host address range 33 to 62
204.15.5.64	255.255.255.224	host address range 65 to 94
204.15.5.96	255.255.255.224	host address range 96 to 126
204.15.5.128	255.255.255.224	host address range 129 to 158
204.15.5.160	255.255.255.224	host address range 161 to 190
204.15.5.192	255.255.255.224	host address range 193 to 222
204.15.5.224	255.255.255.224	host address range 225 to 254

- Using the network subnetting scheme above, which allows for eight subnets, the network might appear as shown in Fig. 3.16.

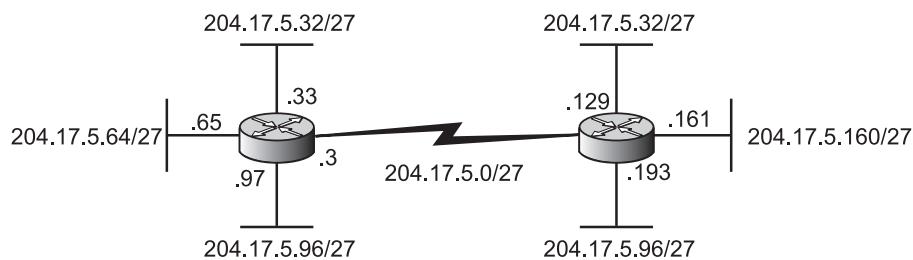


Fig. 3.16

- Fig. 3.17 shows a network using class B addresses before subnetting. In this example we have just one network with almost 216 hosts.
- The whole network is connected, through one single connection, to one of the routers in the Internet.

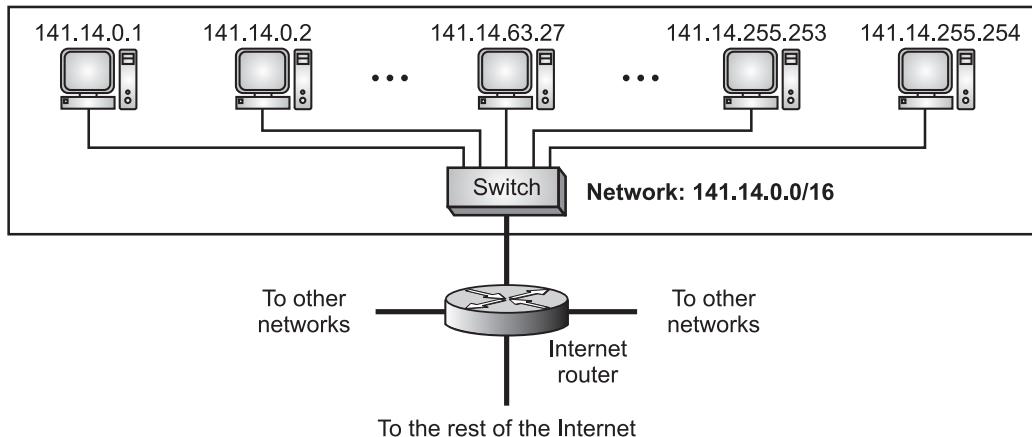


Fig. 3.17

- Fig. 3.18 shows the same network in Fig. 3.17 after subnetting. The whole network is still connected to the Internet through the same router.
- However, the network has used a private router to divide the network into four subnetworks.

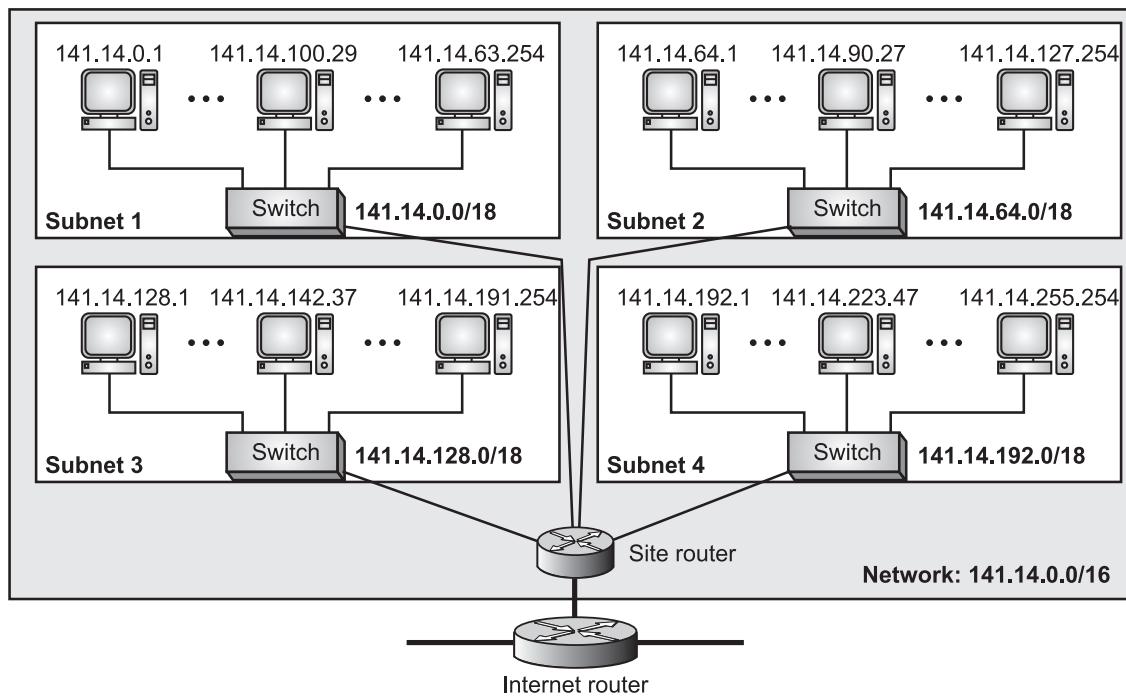


Fig. 3.18

Examples:

Example 1: Assume a company has three offices Central, East, and West. The Central office is connected to the East and West offices via private, point-to-point WAN lines. The company is granted a block of 64 addresses with the beginning address 70.12.100.128/26. The management has decided to allocate 32 addresses for the Central office and divides the rest of addresses between the two other offices.

1. The number of addresses are assigned as follows:

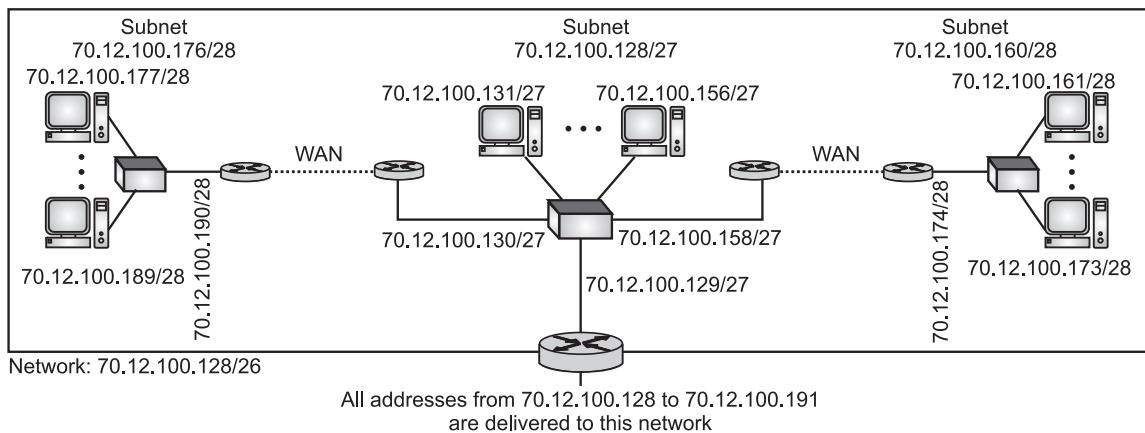
$$\text{Central office } N_c = 32 \quad \text{East office } N_e = 16 \quad \text{West office } N_w = 16$$

2. We can find the prefix length for each subnetwork:

$$n_c = n + \log_2(64/32) = 27 \quad n_e = n + \log_2(64/16) = 28 \quad n_w = n + \log_2(64/16) = 28$$

Solution:

Fig. 3.19 shows the configuration designed by the management. The Central office uses addresses 70.12.100.128/27 to 70.12.100.159/27. The company has used three of these addresses for the routers and has reserved the last address in the subblock. The East office uses the addresses 70.12.100.160/28 to 70.12.100.175/28. One of these addresses is used for the router and the company has reserved the last address in the subblock. The West office uses the addresses 70.12.100.160/28 to 70.12.100.175/28. One of these addresses is used for the router and the company has reserved the last address in the subblock. The company uses no address for the point-to-point connections in WANs.

**Fig. 3.19**

Example 2: An organization is granted the block 130.34.12.64/26. The organization needs four subnetworks, each with an equal number of hosts. Design the subnetworks and find the information about each network.

Solution:

The number of addresses for the whole network can be found as $N = 2^{32-26} = 64$. The first address in the network is 130.34.12.64/26 and the last address is 130.34.12.127/26. We now design the subnetworks:

1. We grant 16 addresses for each subnetwork to meet the first requirement (64/16 is a power of 2).

2. The subnetwork mask for each subnetwork is:

$$n_1 = n_2 = n_3 = n_4 = n + \log_2(N/N_i) = 26 + \log_2 4 = 28$$

3. We grant 16 addresses to each subnet starting from the first available address.

Fig. 3.20 shows the subblock for each subnet. Note that the starting address in each subnetwork is divisible by the number of addresses in the subnetwork.

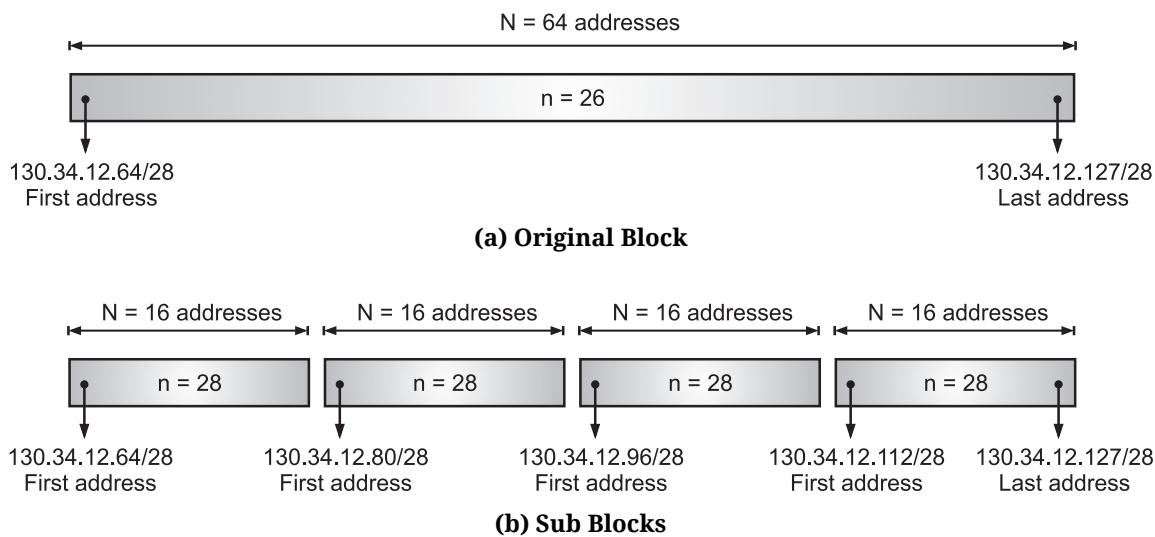


Fig. 3.20

3.3.4 Supernetting

- 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. Supernetting is the 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 supernetwork or a supernet.
- Supernetting, also called Classless Inter-Domain Routing (CIDR), is a way to aggregate multiple Internet addresses of the same class.

- Classful means that the IP addresses and subnets are within the same network. The problem with classful addressing is that there is a lot of unused IP address space.
- For example, a class A IP network has more than 16 million possible host addresses. A Class B network has more than 65,000 host addresses, but the fact is that only a limited number of Class A and B address space has been allocated for Internet use.
- However, the size of a class C block with a maximum number of 256 addresses may not satisfy the needs of an organization. Even a mid-size organization may need more addresses.
- One solution is supernetting. 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 supernet. By doing this, an organization can apply for a set of class C blocks instead of just one.
- For example, an organization that needs 1000 addresses can be granted four class C blocks.
- The organization can then use these addresses in one supernet as shown in Fig. 3.21. When we group two or more classful networks together, they are called supernets.
- The technique supernetting was proposed in 1992 to eliminate the class boundaries and to make available the unused IP address space.
- Supernetting allows multiple networks to be specified by one subnet mask. In other words, the class boundary could be overcome.

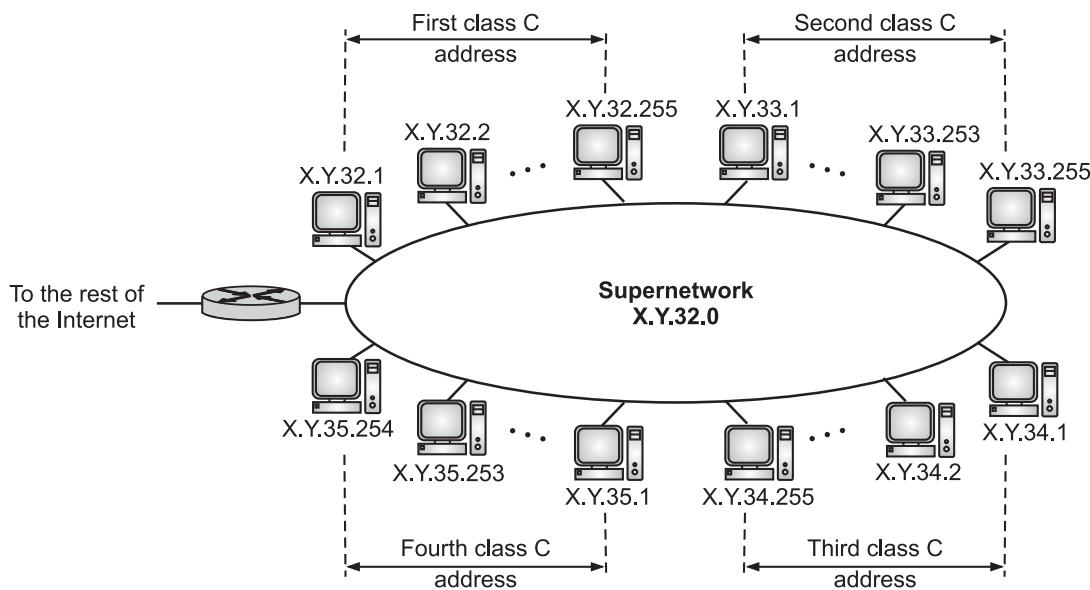


Fig. 3.21: A Supernet

- Supernetting required a simpler way to indicate the subnet mask. The technique developed is called Classless Inter-Domain Routing (CIDR). CIDR notation specifies the number of bits set to a 1 that make up the subnet mask.
- For example, the Class C size subnet mask 255.255.255.0 is listed in CIDR notation as /24. This indicates the 24 bits are set to a 1. A Class B size subnet is written as /16, and a Class A subnet is written as /8.
- CIDR can also be used to represent subnets that identify only part of the octet bits in an IP address. For example, a subnet mask of 255.255.192.0 is written in CIDR as /18.
- The /18 comes from the 18 bits that are set to a 1 as shown below:

255	255	192	0
1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 0 0 0 0 0 0	0 0 0 0 0 0 0 0

- CIDR notation truncates the subnet mask to what is known as “slash” notation. In this example, the network would be identified as 131.107.0.0/16.
- The “/16” value refers to the fact that the first 16 bits in the subnet mask are all set to values of binary 1.

Subnet mask	11111111	11111111	00000000	00000000
	/16			

Fig. 3.22

Advantages of Supernetting:

1. Control and reduce network traffic.
2. Helpful to solve the problem of lacking IP addresses.
3. Minimizes the routing table.

Disadvantages of Supernetting:

1. It cannot cover different areas of the network when combined.
2. All the networks should be in the same class and all IP should be contiguous.

3.3.5 Classless Addressing

- The fast growth of the Internet led to the near depletion of the available addresses. We have run out of class A and B addresses, and a class C addresses is too small for most midsize organizations.
- To overcome the problem of address depletion and give more organizations access to the Internet, classless addressing was designed and implemented.
- In classless addressing, there are no classes, but the addresses are still granted in blocks.
- In 1996, the Internet authorities announced a new architecture called classless addressing. In classless addressing, variable-length blocks are used that belong to no

classes. We can have a block of 1 address, 2 addresses, 4 addresses, 128 addresses, and so on.

- In classless addressing, the whole address space is divided into variable length blocks. Theoretically, we can have a block of $2^0, 2^1, 2^2, \dots, 2^{32}$ addresses. The only restriction, is that the number of addresses in a block needs to be a power of 2. An organization can be granted one block of addresses.
- Fig. 3.23 shows the division of the whole address space into non-overlapping blocks.
- In the classful addressing, routers could just assume the class of an address based on the network ID. In the classless addressing, subnet mask information must always be provided when routers exchange information with each other.
- Some routing protocols, such as the Border Gateway Protocol (BGPv4) and OSPF, support classless addressing.

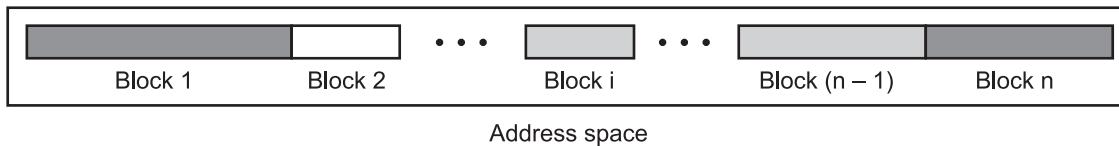


Fig. 3.23: Variable Length Blocks in Classless Addressing

- In classless addressing, when an entity, small or large, needs to be connected to the Internet, it is granted a block or range of addresses.
- The size of the block (the number of addresses) varies based on the nature and size of the entry.
- For example, a household may be given only two addresses; a large organization may be given thousands of addresses. An ISP, may be given thousands or hundreds of thousands based on the number of customers it may serve.
- In classless addressing variable-length blocks are assigned that belong to no class. In this architecture, the entire address space (2³² addresses) is divided into blocks of different sizes.
- All IP addresses have a network and host portion. Classless addressing uses a variable number of bits for the host portions of the address.

Decimal	192	160	20	48
Binary	11000000	10100000	00010100	00110000

←———— 28 bits network —————→ 4 bits host

- Classless addressing treats the IP address as a 32-bits stream of ones and zeros, where the boundary between network and host portion can fall anywhere between bit 0 and bit 31.

- The network portion of an IP address is determined by how many 1's are in the subnet mask. Again, this can be a variable number of bits, and although it can fall on an octet boundary, it does not necessarily need to.

3.3.6 Network Address Translation (NAT)

- The number of home users and small businesses who want to use the Internet is day-by-day increasing. ISP assigns a block of addresses to its user. An address is assigned to a user when it is needed.
- 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).
- A technology that can provide the mapping between the private and universal addresses, and at the same time support Virtual Private Networks (VPNs) is Network Address Translation (NAT).
- The NAT technology allows a site to use a set of private addresses for internal communication and a set of global Internet addresses (at least one) for communication with the rest of the world.
- The site must have only one connection to the global Internet through a NAT-capable router that runs NAT software.
- Fig. 3.24 shows a simple implementation of NAT. NAT is a method of remapping one IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device.
- The technique was originally used as a shortcut to avoid the need to readdress every host when a network was moved.

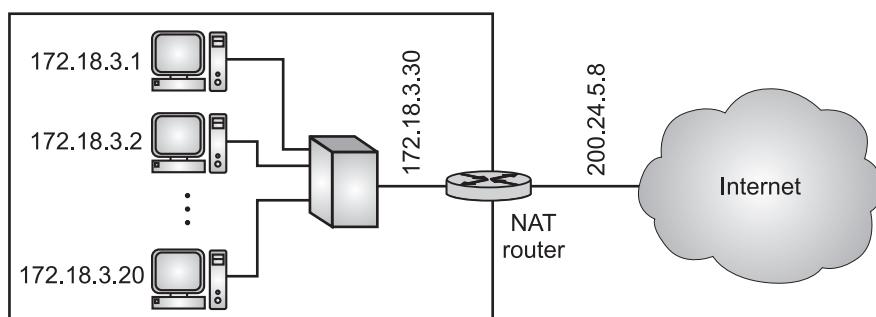


Fig. 3.24

- As the Fig. 3.24 shows, the private network uses private addresses.
- The router that connects the network to the global address uses one private address and one global address. The private network is invisible to the rest of the Internet; the rest of the Internet sees only the NAT router with the address 200.24.5.8.

Concept of Address Translation:

- NAT is a process in which one or more local IP addresses are translated into one or more Global IP addresses and vice versa in order to provide Internet access to the local hosts.
- NAT translates the IP addresses of computers in a local network to a single IP address. This address is often used by the router that connects the computers to the Internet.
- All of the outgoing packets go through the NAT router, which replaces the source address in the packet with the global NAT address.
- All incoming packets also pass through the NAT router, which replaces the destination address in the packet (the NAT router global address) with the appropriate private address.
- Fig. 3.25 shows an example of address translation.

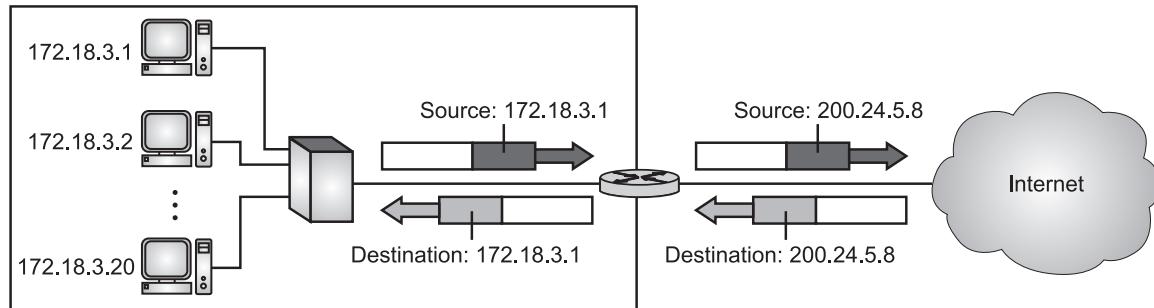


Fig. 3.25: Address Translation

Translation Table:

- The reader may have noticed that translating the source addresses for an outgoing packet is straightforward. But how does the NAT router know the destination address for a packet coming from the Internet? There may be tens or hundreds of private IP addresses, each belonging to one specific host. The problem is solved if the NAT router has a translation table.
- The NAT table is what allows devices on a private network to access a public network, such as the internet.
- A NAT table is a table of network address translations, where each row in the table is basically a mapping from one private address to one public address.

Using One IP Address:

- In its simplest form, a translation table has only two columns namely the private address and the external address (destination address of the packet).
- When the router translates 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. 3.26 shows the idea.

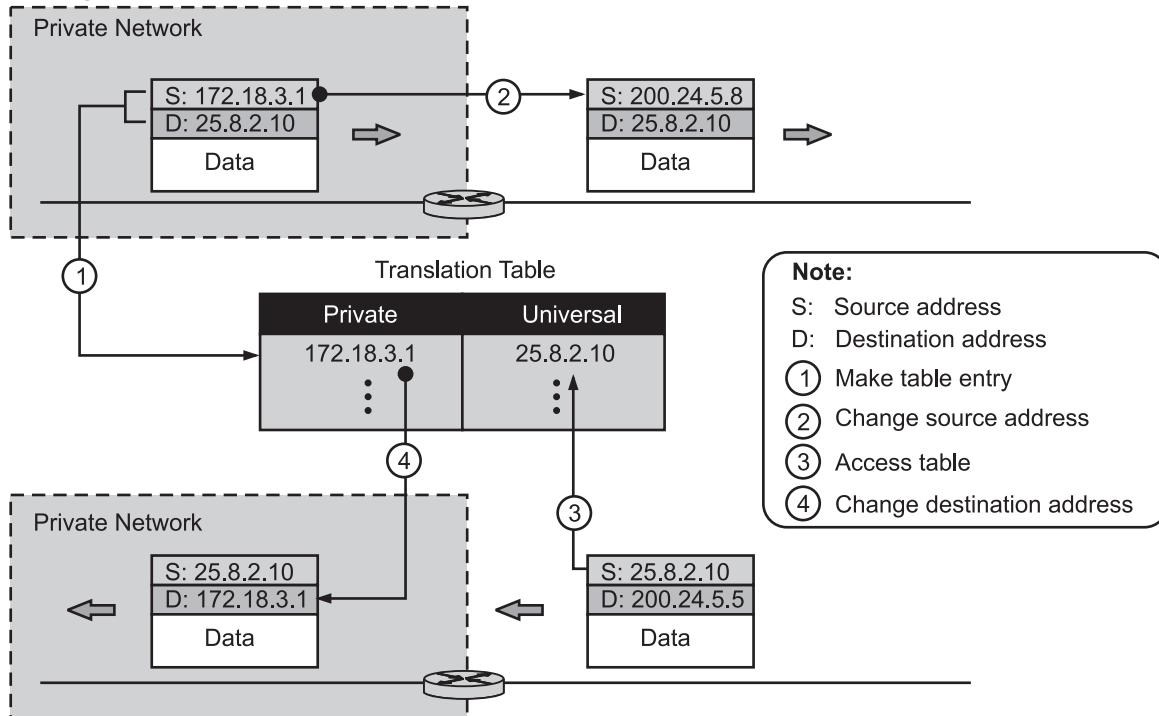


Fig. 3.26

Using a Pool of IP Addresses:

- The use of only one global address by the NAT router allows only one private-network host to access a given external host. To remove this restriction, the NAT router can use 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 separate connection.

Using Both IP Addresses and Port Addresses:

- To allow 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 an 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 3.1 shows an example of such a table.

Table 3.1: 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
...

Advantages of NAT:

1. NAT solves IP overlapping issues.
2. NAT hides internal IP structure from the external world.
3. NAT allows us to connect with any network without changing IP address.
4. NAT allows connecting multiple computers with the internet through the single public IP address.

Disadvantages of NAT:

1. NAT adds additional delay in the network.
2. Several applications are not compatible with NAT.
3. End to end IP traceability will not work with NAT.
4. NAT hides the actual end device.

3.4 FORWARDING OF IP PACKETS

- Forwarding means to place the packet in its route to its destination. Since, the Internet today is made of a combination of links (networks), forwarding means to deliver the packet to the next hop (which can be the final destination or the intermediate connecting device).
- Although the IP protocol was originally designed as a connection less protocol, today the tendency is to change it to connection-oriented protocol.
- When IP is used as a connection less protocol, forwarding is based on the destination address of the IP datagram when the IP is used as a connection oriented protocol, forwarding is based on the label attached to an IP datagram.

3.4.1 Forwarding Based on Destination Address

- Forwarding IP packets based on the destination address is a traditional approach, which is prevalent today.

- In this case, forwarding requires a host or a router to have a forwarding table. When a host has a packet to send or when a router has received a packet to be forwarded, it looks at this table to find the next hop to deliver the packet to.
- In classless addressing, the whole address space is one entity; there are no classes. This means that forwarding requires one row of information for each block involved.
- The table needs to be searched based on the network address (first address in the block). Unfortunately, the destination address in the packet gives no clue about the network address.
- To solve the problem, we need to include the mask (/n) in the table. In other words, a classless forwarding table needs to include four pieces of information: the mask, the network address, the interface number, and the IP address of the next router (needed to find the link-layer address of the next hop).
- However, we often see in the literature that the first two pieces are combined. For example, if n is 26 and the network address is 180.70.65.192, then one can combine the two as one piece of information: 180.70.65.192/26.
- Fig. 3.27 shows a simple forwarding module and forwarding table for a router with only three interfaces.

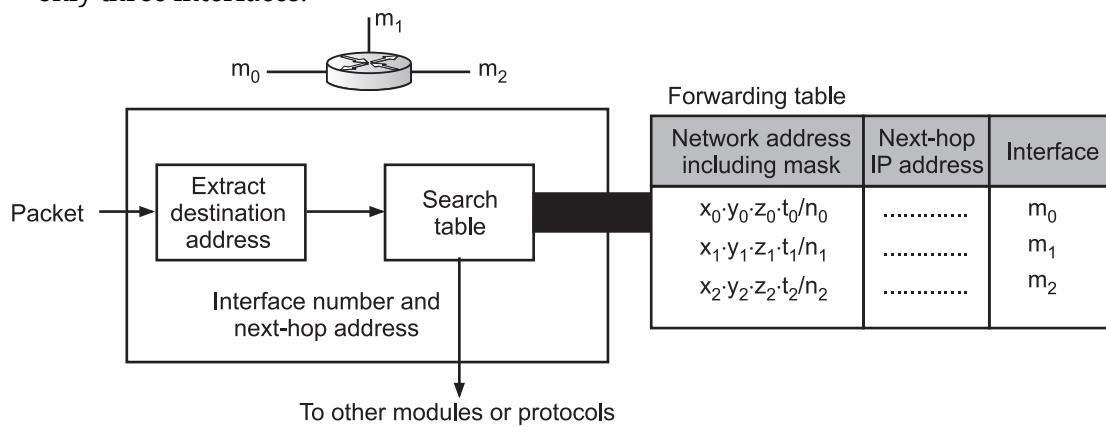


Fig. 3.27: Simplified Forwarding Module in Classless Address

- The job of the forwarding module is to search the table, row by row. In each row, the n leftmost bits of the destination address (prefix) are kept and the rest of the bits (suffix) are set to 0s.
- If the resulting address (which we call the network address), matches with the address in the first column, the information in the next two columns is extracted; otherwise the search continues.
- Normally, the last row has a default value in the first column (not shown in Fig. 3.27), which indicates all destination addresses that did not match the previous rows.

- Sometimes, the literature explicitly shows the value of the n leftmost bits that should be matched with the n leftmost bits of the destination address.
- The concept is the same, but the presentation is different. For example, instead of giving the address-mask combination of 180.70.65.192/26, we can give the value of the 26 leftmost bits as shown below:

10110100 01000110 01000001 11

- Note that we still need to use an algorithm to find the prefix and compare it with the bit pattern.
- In other words, the algorithm is still needed, but the presentation is different. We use this format in our forwarding tables in the exercises when we use smaller address spaces just for practice.
- For example, make a forwarding table for router R1 using the configuration in Fig. 3.28.

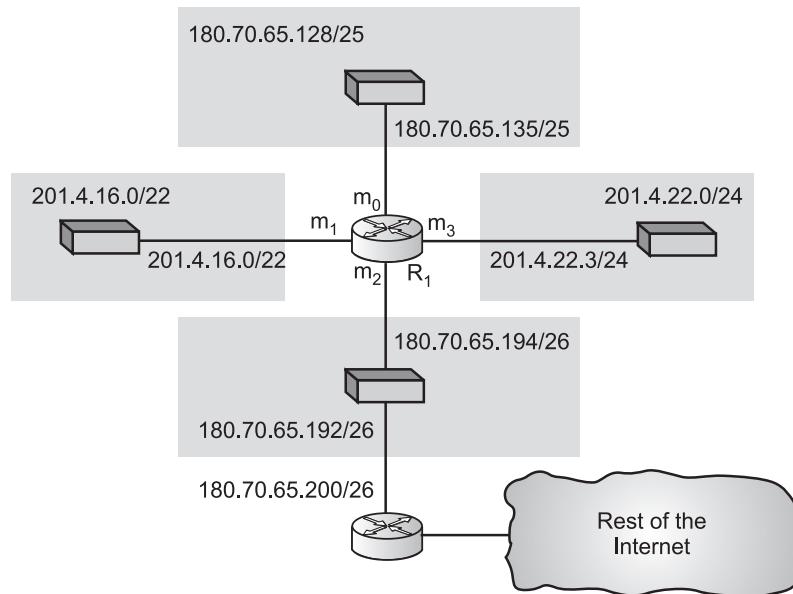


Fig. 3.28

Solution: Table 3.2 shows the corresponding table.

Table 3.2: Forwarding table for router R1 in Fig. 3.28

Network Address/Mask	Next Hop	Interface
180.70.65.192/26	-	m_2
180.70.65.128/25	-	m_0
201.4.22.0/24	-	m_3
201.4.16.0/22	-	m_1
Default	180.70.65.200	m_2

- Fig. 3.29 showed a simple example of searching in a forwarding table using the longest mask algorithm. Although there are some more efficient algorithms today, the principle is the same.
- When the forwarding algorithm gets the destination address of the packet, it needs to delve into the mask column.
- For each entry, it needs to apply the mask to find the destination network address. It then needs to check the network addresses in the table until it finds the match.
- The router then extracts the next-hop address and the interface number to be delivered to the data-link layer.

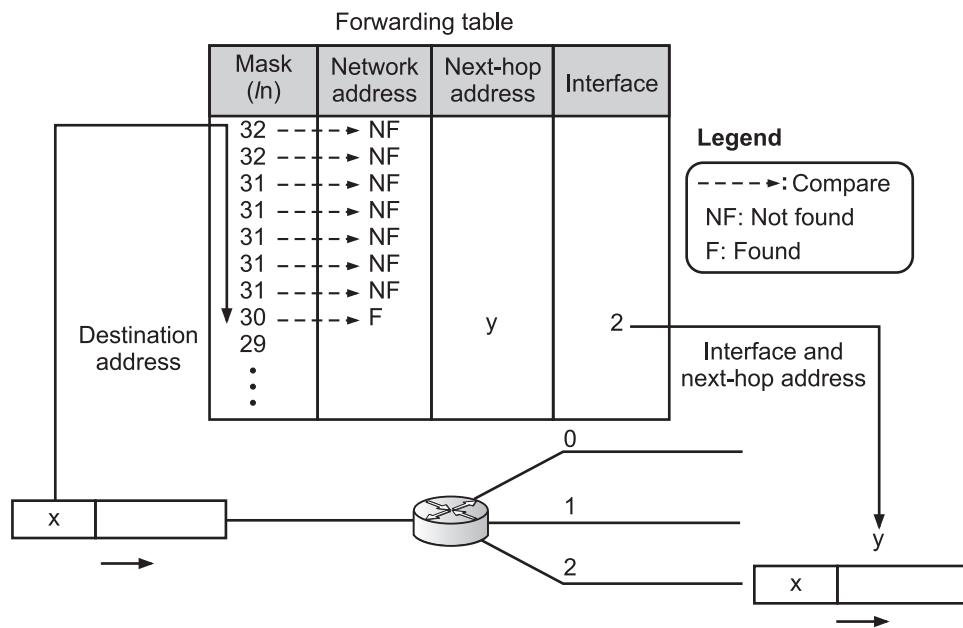


Fig. 3.29: Forwarding Based on Destination Address

3.4.2 Forwarding Based on Label

- In the 1980s, an effort started to somehow change IP to behave like a connection oriented protocol in which the routing is replaced by switching.
- In a connectionless network (datagram approach), a router forwards a packet based on the destination address in the header of the packet.
- On the other hand, in a connection-oriented network (virtual-circuit approach), a switch forwards a packet based on the label attached to the packet.
- Routing is normally based on searching the contents on a table; switching can be done by accessing a table using an index. In other words, routing involves searching; switching involves accessing.

- Fig. 3.30 shows a simple example of using a label to access a switching table. Since, the labels are used as the index to the table, finding the information in the table is immediate.

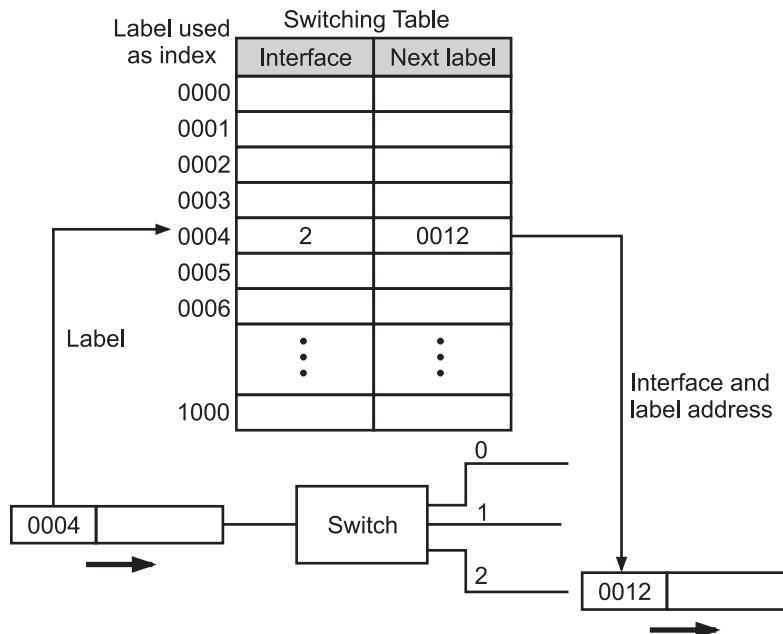


Fig. 3.30: Forwarding Based on Label

- During the 1980s several vendors created routers that implement switching technology.
- In standard Multiple Protocol Label Switching (MLPS) conventional routers in the Internet can be replaced by MPLS routers, which can behave like a router and a switch.
- When behaving like a router, MPLS can forward the packet based on the destination address; when behaving like a switch, it can forward a packet based on the label.

3.5 NETWORK LAYER PROTOCOLS

- Fig. 3.31 shows the positions of the network layer protocols in the TCP/IP protocol suite.
- In network layer, Internet Protocol version 4 (IPv4), is responsible for forwarding, packetizing, and delivery of a packet.
- The Internet Control Message Protocol version 4 (ICMPv4) helps IPv4 to handle some errors that may occur in the network-layer delivery.
- The Internet Group Management Protocol (IGMP) is used to help IPv4 in multicasting.

- The Address Resolution Protocol (ARP) is used to glue the network and data-link layers in mapping network-layer addresses to link-layer addresses.

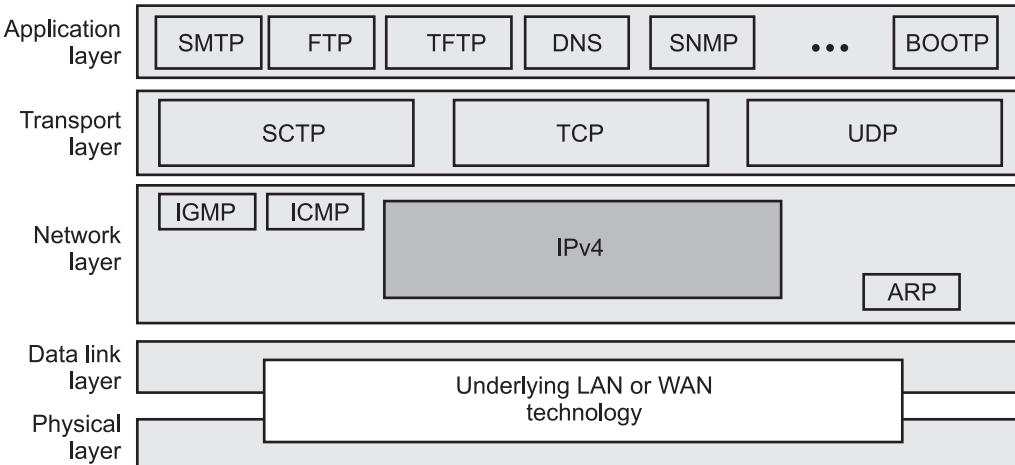


Fig. 3.31: Positions of Network Layer Protocols in TCP/IP Protocol Suite

3.5.1 Internet Protocol (IP)

- The Internet Protocol (IP) is a protocol or set of rules, for routing and addressing packets of data so that they can travel across networks and arrive at the correct destination.
- IP is an unreliable and connection less datagram protocol. Internet Protocol works at the network layer.
- Internet Protocol (IP) has the responsibility of identifying hosts based upon their logical addresses and to route data among them over the underlying network.
- IP provides a mechanism to uniquely identify hosts by an IP addressing scheme. IP uses best effort delivery, i.e. it does not guarantee that packets would be delivered to the destined host, but it will do its best to reach the destination.
- There are two versions of IP that currently coexist in the Internet namely, IP version 4 (IPv4) and IP version 6 (IPv6).
- Internet Protocol version 4 (IPv4) is the fourth version of the Internet Protocol (IP).
- IPv4 is one of the core protocols of standards-based internetworking methods in the Internet and other packet-switched networks. Internet Protocol version 4 uses 32-bit logical 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. Internet Protocol version 6 uses a 128-bit logical address.

- In this section we will study Internet Protocol version 4 (IPv4) which is a widely used protocol in data communication over different kinds of networks as a delivery of packets.
- 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 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.

3.5.2 IPv4 Datagram Format

- In IPv4, packets are called datagram, which is a basic transfer unit associated with a packet-switched network.
- The IP datagram format is shown in Fig. 3.32.

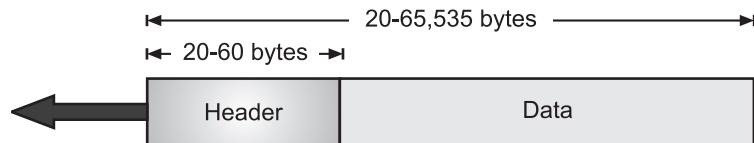


Fig. 3.32: IP Datagram

- A datagram is a variable-length packet consisting of two parts namely, header and data.
- The header is 20 to 60 bytes in length and contains information essential to routing and delivery.

Header Format:

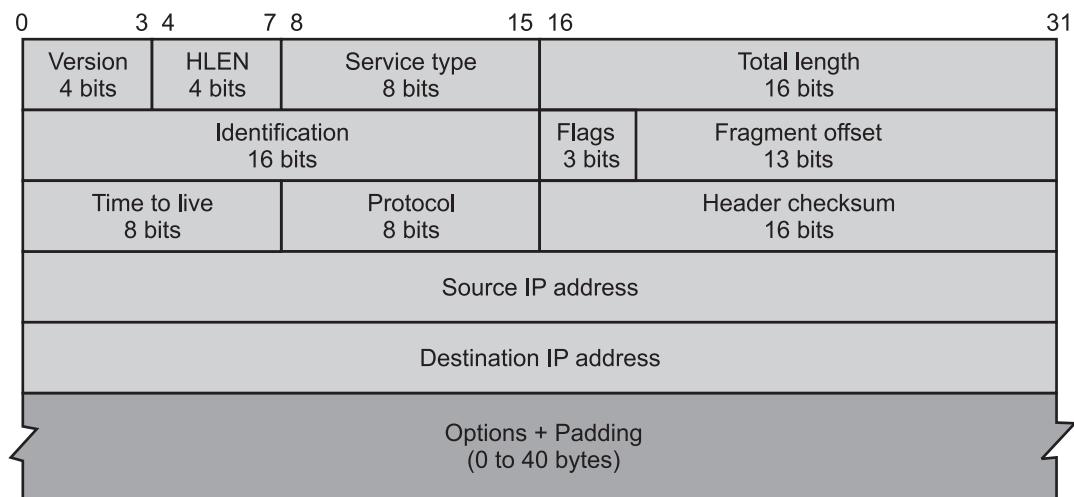


Fig. 3.33: Header Format

- A 20-byte header contains almost 13 multipurpose fields, which hold specific related object information such as application, data type and source/destination addresses.
- IP header format contains following fields:
 - Version (VER):** This 4-bits field defines the current version of IP protocol. Currently the IP version is 4 (IPv4). 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. However, IP version 6 (IPv6) may replace version 4 in the future.
 - Header Length (HLEN):** This 4-bits 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($5 \times 4 = 20$). When the option field is at its maximum size, the value of this field is 15($15 \times 4 = 60$).
 - Service Type:** This 8-bits field previously known as service type, is now called differentiated services. Both implementations are shown in Fig. 3.34.

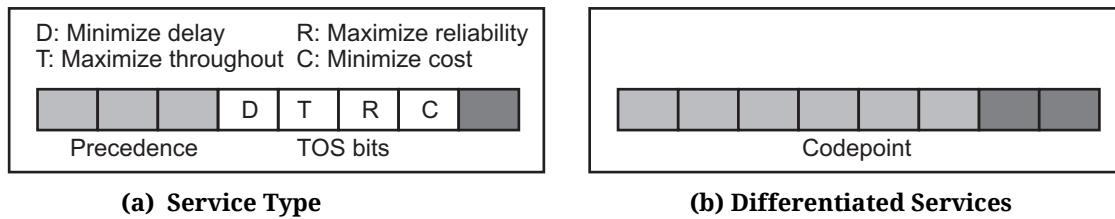


Fig. 3.34

- (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 3-bits 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-bits subfield defines types of services. We can have 5 different types of services as listed in the following table.

Table 3.3: 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 code-point 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.

$$\text{Length of data} = \text{Total length} - \text{Header length}$$

5. **Identification:** This 16-bits field contains a specific number for primary data identification. Uniquely identifies the datagram. Usually incremented by 1 each time a datagram is sent. All fragments of a datagram contain the same identification value. This allows the destination host to determine which fragment belongs to which datagram. This field is used in fragmentation.
6. **Flags (3-bits):** As required by the network resources, if the IP packet is too large to handle, these ‘flags’ tell if they can be fragmented or not. This router fragment activity is controlled by following three flags:

Sr. No.	Flag	Description
1.	0	Reserved, must be zero.
2.	DF (Do not Fragment)	0 means allow fragmentation; 1 means do not allow fragmentation.
3.	MF (More Fragments)	0 means that this is the last fragment of the datagram; 1 means that additional fragments will follow.

7. **Fragmentation Offset:** This 13-bits offset tells the exact position of the fragment in the original IP packet. This field is used in fragmentation.
8. **Time To Live (TTL) (8 bit):** Every datagram has a limited lifetime on the Internet. This field is used to control the maximum number of hops (routers) visited by the datagram. To avoid looping in the network, every packet is sent with some TTL value set, which tells the network how many routers (hops) this packet can cross. At each hop, its value is decremented by one and when the value reaches zero, the packet is discarded.
9. **Protocol:** This 8-bits 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. **Header Checksum:** This 18-bits field is used for error detection.
11. **Source address:** This 32-bits field defines the source address of a datagram.
12. **Destination address:** This 32-bits field defines the destination address of a datagram.
13. **Options:** This optional field may contain values for options such as Security, Record Route, Time Stamp, etc.

3.5.3 Fragmentation

(Oct. 17, 18)

- To reach up to 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.

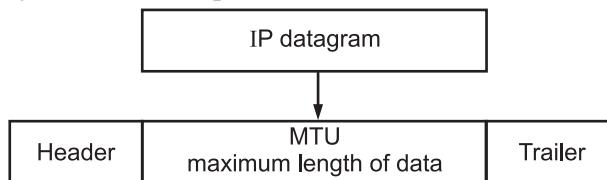


Fig. 3.35: Maximum Transfer Unit (MTU)

Table 3.4: MTU for some networks

Protocol	MTU
Hyper-channel	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-bits 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:

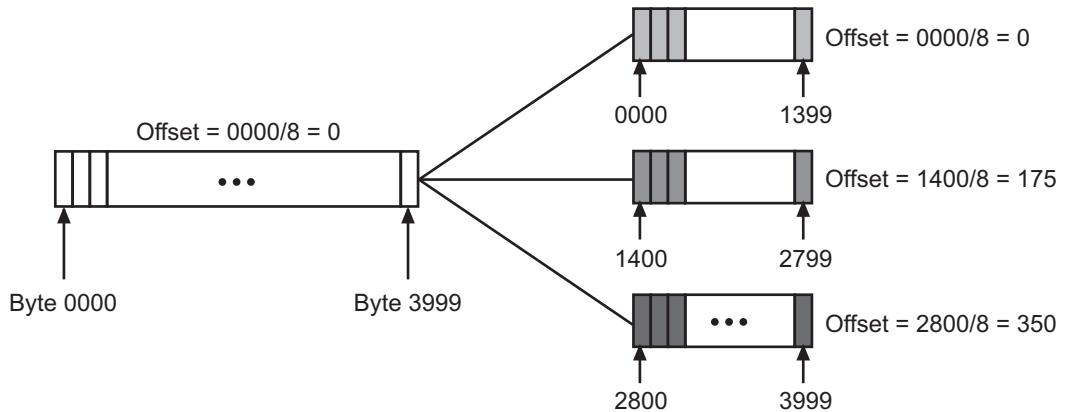
- From the 3-bits, the first bit is reserved.
- The second bit is called the do not fragment bit. If its value is 1, the machine must not fragment the datagram. If it cannot pass the datagram, it must discard it. If the value is 0, the datagram can be fragmented if necessary.
- The third bit is called 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.



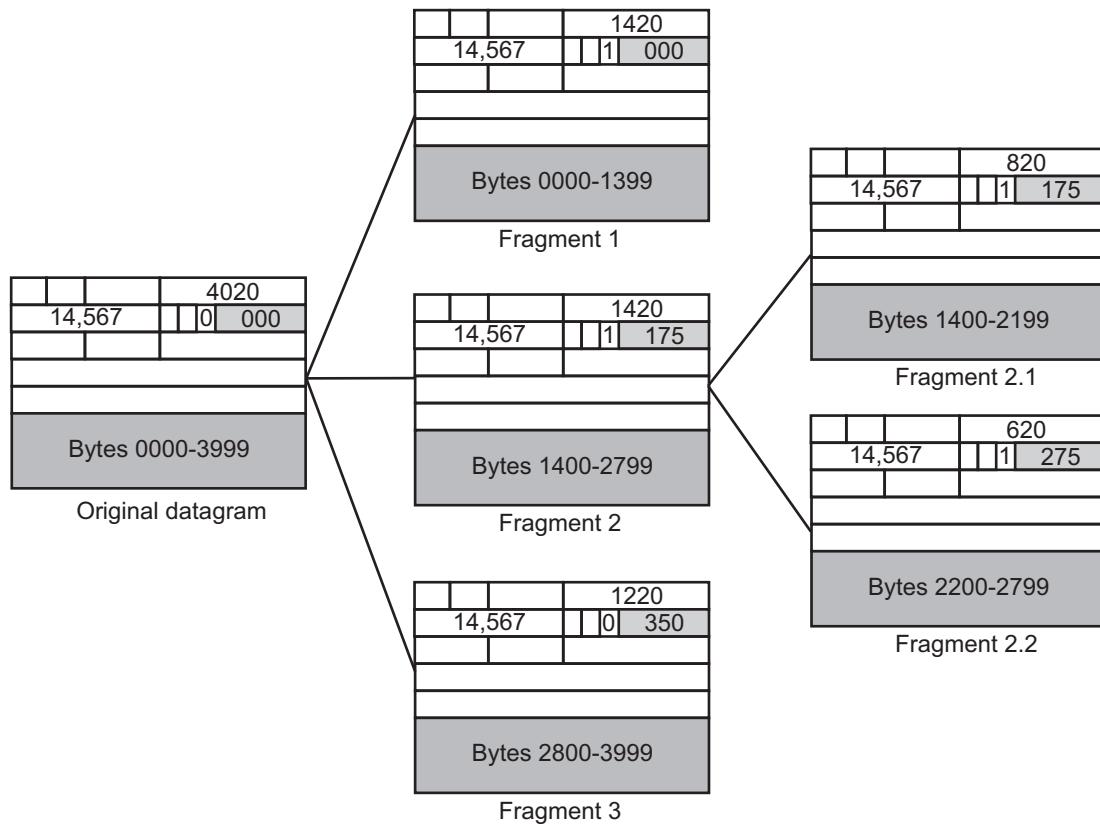
Fig. 3.36: Flags used in Fragmentation

3. Fragmentation Offset:

- This 13-bits field shows the position of the fragment with respect to the whole datagram.
- Fig. 3.37 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 $\frac{0}{8} = 0$. The second fragment carries 1400 to 2799, the offset is $\frac{1400}{8} = 8 = 175$. The third one carries 2800 to 3999 bytes. The offset value is $\frac{2800}{8} = 350$.

**Fig. 3.37: Example of Fragmentation**

- Fig. 3.38 shows an expanded view of the fragments in Fig. 3.37.

**Fig. 3.38: Detailed Example of Fragmentation**

3.5.4 Options

- The header of the IP datagram is made of two parts namely, a fixed part and a variable part.
- The fixed part is 20 bytes long, and the variable part comprises the options, which can be a maximum of 40 bytes.
- Options, as the name implies, are not required for a datagram. They can be used for network testing and debugging.
- Fig. 3.39 shows the format of an option.

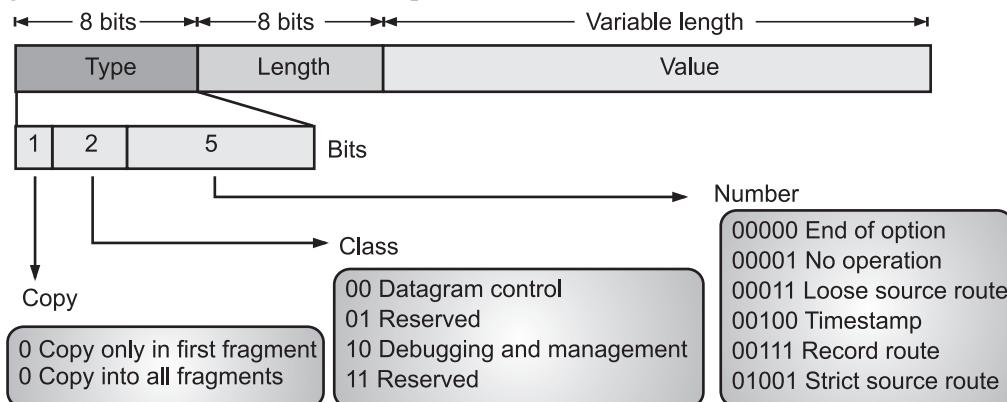


Fig. 3.39: Option Format

- The various field in option format are explained below:
 - Type:** The type field is 8-bits long and contains three subfields namely, copy, class, and number.
 - Copy:** This 1-bits subfield controls the presence of the option in fragmentation. When its value is 0, it means that the option must be copied only to the first fragment. If its value is 1, it means the option must be copied to all fragments.
 - Class:** This 2-bits subfield defines the general purpose of the option. When its value is 00, it means that the option is used for datagram control. When its value is 10, it means that the option is used for debugging and management. The other two possible values (01 and 11) have not yet been defined.
 - Number:** This 5-bits subfield defines the type of option. Although 5 bits can define up to 32 different types, currently only 6 types are in use.
 - Length:** The length field defines the total length of the option including the type field and the length field itself. This field is not present in all of the option types.
 - Value:** The value field contains the data that specific options require. Like the length field, this field is also not present in all option types.

Options Types:

- Fig. 3.40 shows types of options.
- Options are not required for a datagram, they are used for network testing and debugging.

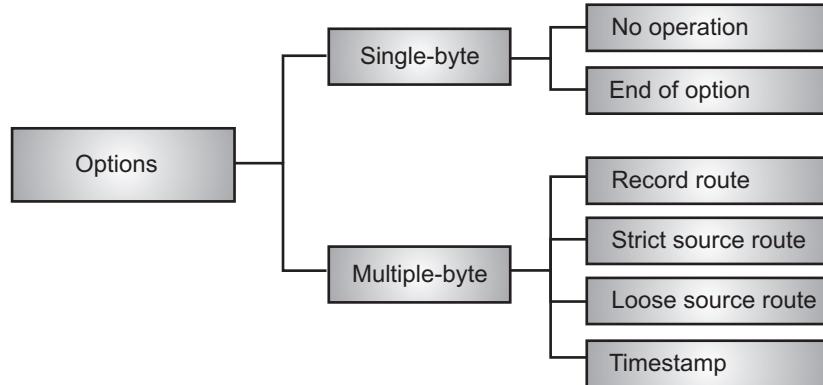


Fig. 3.40: Options in IPv4

- Various options in IPv4 are explained below:
 - No Operation Option:** A no-operation option is a 1-byte option used as a filler between options.
 - End of Option:** An end-of-option 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.
 - Record Route Option:** A record route option is used to record the Internet routers that handle the datagram. It can list up to nine router addresses.
 - Strict Source Route Option:** 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.
 - Loose Source Route Option:** 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.
 - Timestamp Option:** A timestamp option is used to record the time of datagram processing by a router. This can help users and managers to track the behavior of the routers on the Internet. We can estimate time taken for a datagram to go from one router to another.

3.6 MOBILE IP

- In the last decade, mobile communication has received a lot of attention. The interest in mobile communication on the Internet means that the IP protocol, originally designed for stationary devices, must be enhanced to allow the use of mobile computers, computers that move from one network to another.
- Mobile IP (MIP) is an Internet Engineering Task Force (IETF) standard communications protocol that is designed to allow mobile device users to move from one network to another while maintaining a permanent IP address.
- The goals of a Mobile IP include supporting end-system mobility while maintaining scalability, efficiency, and compatibility in all respects with existing applications and Internet protocols.
- Mobile IP communication protocol refers to the forwarding of Internet traffic with a fixed IP address even outside the home network. It allows users having wireless or mobile devices to use the Internet remotely.
- Mobile IP for IPv4 is described in IETF RFC 5944, and extensions are defined in IETF RFC 4721.
- Mobile IPv6, the IP mobility implementation for the next generation of the Internet Protocol, IPv6 is described in RFC 6275.

3.6.1 Architecture of Mobile IP

- The objective of IP mobility is to maintain the TCP connection between a mobile host and a static host while reducing the effects of location changes while the mobile host is moving around, without having to change the underlying TCP/IP.
- The Mobile IP allows for location-independent routing of IP datagrams on the Internet. Each mobile node is identified by its home address disregarding its current location in the Internet.
- While away from its home network, a mobile node is associated with a care-of address which identifies its current location and its home address is associated with the local endpoint of a tunnel to its home agent.
- Mobile IP specifies how a mobile node registers with its home agent and how the home agent routes datagrams to the mobile node through the tunnel.
- A mobile node has two addresses, a permanent home address and a Care-of Address (CoA), which is associated with the network the mobile node is visiting.
- The home network of a mobile device is the network within which the device receives its identifying IP address (home address). The home address of a mobile device is the IP address assigned to the device within its home network.
- The network node that is responsible for forwarding and managing this transparency is known as the home agent.

- A Home Agent (HA) stores information about mobile nodes whose permanent home address is in the home agent's network.
- The HA acts as a router on a Mobile Host's (MH) home network which tunnels datagrams for delivery to the MH when it is away from home, maintains a Location Directory (LD) for the MH.
- A Foreign Agent (FA) stores information about mobile nodes visiting its network. Foreign agents also advertise care of addresses, which are used by Mobile IP.
- If there is no foreign agent in the host network, the mobile device has to take care of getting an address and advertising that address by its own means.
- A Mobile Node (MN) is responsible for discovering whether it is connected to its home network or has moved to a foreign network. HA's and FA's broadcast their presence on each network to which they are attached.
- A foreign network is the network in which a mobile node is operating when away from its home network.
- Whenever the mobile node moves, it registers its new care of address with its home agent. The home agent forwards the packet to the foreign network using the care of address.
- The delivery requires that the packet header is modified so that the care of address becomes the destination IP address.
- This new header (See Fig. 3.42) encapsulates the original packet, causing the mobile node's home address to have no impact on the encapsulated packet's routing. This phenomenon is called tunneling.
- Fig. 3.41 shows architecture of Mobile IP.

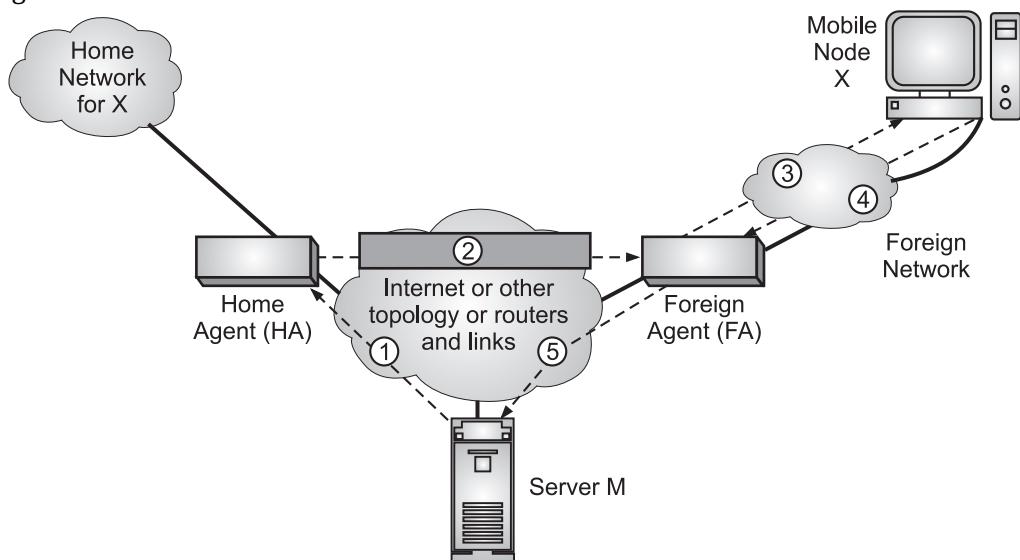
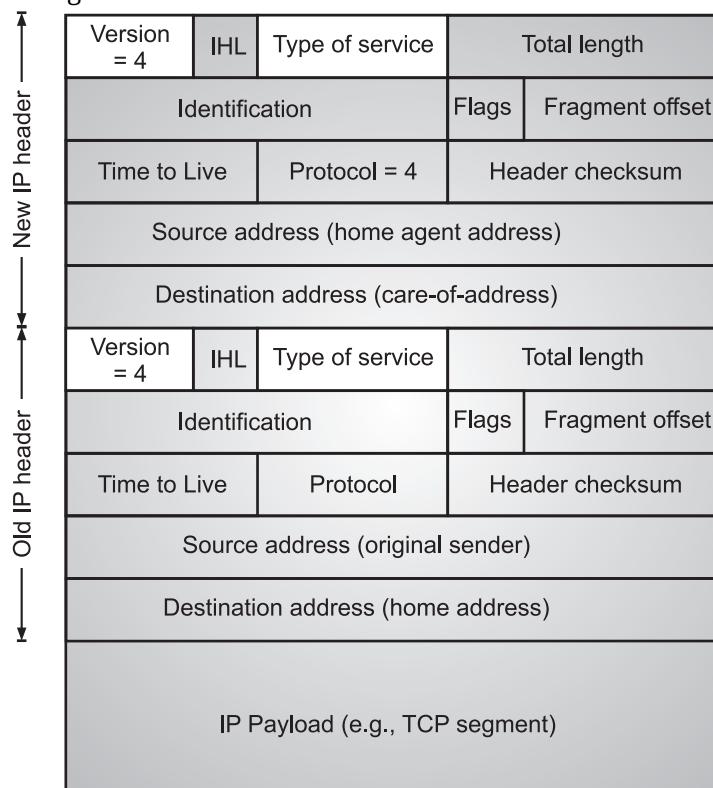


Fig. 3.41: Mobile IP Architecture

- Let us take an example of IP datagrams being exchanged over a TCP connection between the mobile node (X) and another host (server M in Fig. 3.41), the following steps occur:

Step 1: Server M wants to transmit an IP datagram to node X. The home address of X is advertised and known to M. M does not know whether X is in the home network or somewhere else. Therefore, M sends the packet to X with X's home address as the destination IP address in the IP header. The IP datagram is routed to X's home network.

Step 2: At the X's home network, the incoming IP datagram is intercepted by the home agent. The home agent discovers that X is in a foreign network. A care of address has been allocated to X by this foreign network and available with the home agent. The home agent encapsulates the entire datagram inside a new IP datagram, with X's care of address in the IP header. This new datagram with the care of address as the destination address is retransmitted by the home agent.



Note: Unshaded fields are copied from the inner IP header to the outer IP header.

Fig. 3.42: The IP Headers in Mobile IP (IP Encapsulation)

Step 3: At the foreign network, the incoming IP datagram is intercepted by the foreign agent. The foreign agent is the counterpart of the home agent in the foreign network. The foreign agent strips off the outer IP header, and delivers the original datagram to X.

Step 4: A intends to respond to this message and sends traffic to M. In this example, M is not mobile; therefore M has a fixed IP address. For routing X's IP datagram to M, each datagram is sent to some router in the foreign network. Typically, this router is the foreign agent. X uses M's IP static address as the destination address in the IP header.

Step 5: The IP datagram from X to M travels directly across the network, using M's IP address as the destination address.

- To support the operations illustrated in the previous example, mobile IP needs to support following three basic capabilities/functions:
 1. **Discovery:** A mobile node uses a discovery procedure to identify prospective home agents and foreign agents.
 2. **Registration:** A mobile node uses a registration procedure to inform its home agent of its care-of address.
 3. **Tunneling:** Tunneling procedure is used to forward IP datagrams from a home address to a care-of address.

3.6.2 Addressing

- The main problem that must be solved in providing mobile communication using the IP protocol is addressing.

Stationary Hosts:

- The original IP addressing was based on the assumption that a host is stationary, attached to one specific network. A router uses an IP address to route an IP datagram.
 - An IP address has two parts namely, a prefix and a suffix. The prefix associates a host to a network. For example, the IP address 10.3.4.24/8 defines a host attached to the network 10.0.0.0/8. This implies that a host on the Internet does not have an address that it can carry with itself from one place to another.
 - The address is valid only when the host is attached to the network. If the network changes, the address is no longer valid.
 - Routers use this association to route a packet; they use the prefix to deliver the packet to the network to which the host is attached. This scheme works perfectly with stationary hosts.
1. **Mobile Hosts:** When a host moves from one network to another, the IP addressing structure needs to be modified. The solutions are:

- 2. Changing the Address:** One simple solution is to let the mobile host change its address as it goes to the new network. The host can use DHCP to obtain a new address to associate it with the new network. This approach has several drawbacks.
- (i) First, the configuration files would need to be changed.
 - (ii) Second, each time the computer moves from one network to another, it must be rebooted.
 - (iii) Third, the DNS tables need to be revised so that every other host in the Internet is aware of the change.
 - (iv) Fourth, if the host roams from one network to another during a transmission, the data exchange will be interrupted.
 - This is because the ports and IP addresses of the client and the server must remain constant for the duration of the connection.

Two Addresses:

- The approach that is more feasible is the use of two addresses. The host has its original address, called the home address, and a temporary address, called the care-of address.
- The home address is permanent; it associates the host to its home network, the network that is the permanent home of the host.
- The care of address is temporary. When a host moves from one network to another, the care-of address changes; it is associated with the foreign network, the network to which the host moves.

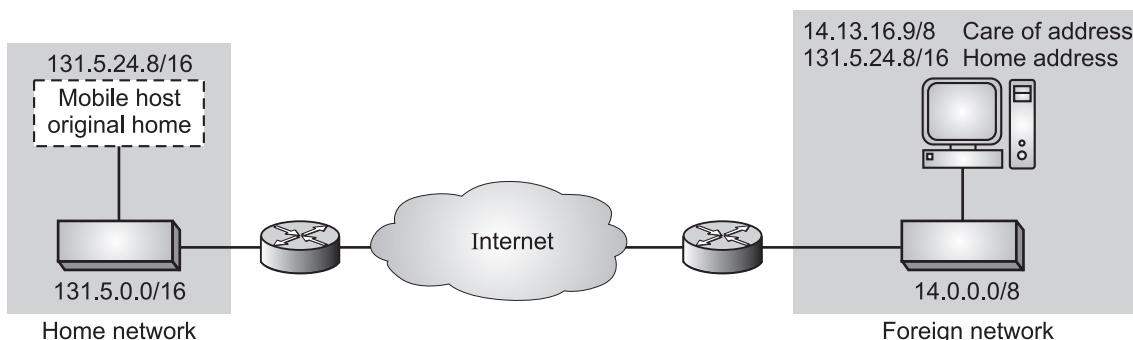


Fig. 3.43: Home Address and Care of Address (CoA)

3.6.3 Agents

- Mobile IP enables the transfer of information to and from mobile computers, such as laptops and wireless communications.
- To make the change of address transparent to the rest of the Internet requires a home agent and a foreign agent.

- Fig. 3.44 shows the position of a home agent relative to the home network and a foreign agent relative to the foreign network.
 - Home network is a network to which the mobile node originally belongs to as per its assigned IP address (home address). Foreign Network is the current network to which the mobile node is visiting (away from its home network).
 - Fig. 3.44 shows Home Agent (HA) and Foreign Agent (FA).
- Home Agent:** The home agent is usually a router attached to the home network of the mobile host. The HA acts on behalf of the mobile host when a remote host sends a packet to the mobile host. The home agent receives the packet and sends it to the foreign agent.
 - Foreign Agent:** The foreign agent is usually a router attached to the foreign network. The FA receives packets sent by the home agent and deliver them to the mobile host.

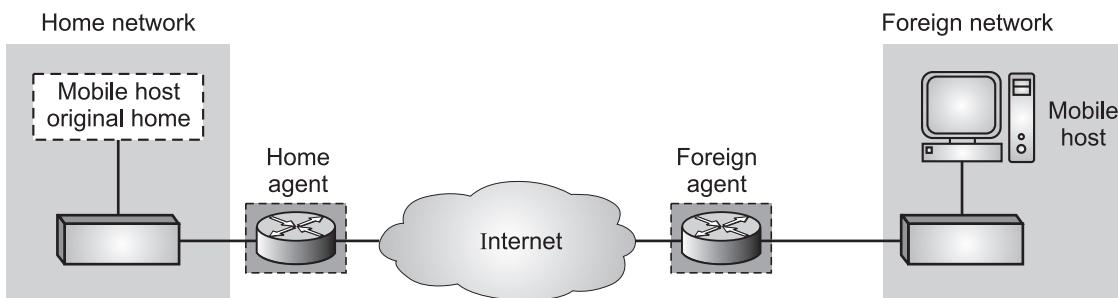


Fig. 3.44: Home Agent (HA) and Foreign Agent (FA)

3.6.4 Three Phases

- To communicate with a remote host, a mobile host goes through three phases namely, agent discovery, registration and data transfer.
- Fig. 3.45 shows the three phases, agent discovery (involves the mobile host, the foreign agent and the home agent) registration (also involves the mobile host and the two agents) and data transfer (remote host is also involved).
- The Mobile IP process has three main phases as explained below:

Phase I: Agent Discovery:

- This is the first phase of the mobile IP process, where mobile nodes discover its foreign agents and home agents.
- The agent discovery phase, consists of following two sub phases:
 - A mobile host must discover (learn the address of) a home agent before it leaves its home network.

2. A mobile host must also discover a foreign agent after it has moved to a foreign network. This discovery consists of learning the care of address as well as the foreign agent's address.
- The discovery involves two types of messages namely, advertisement and solicitation.

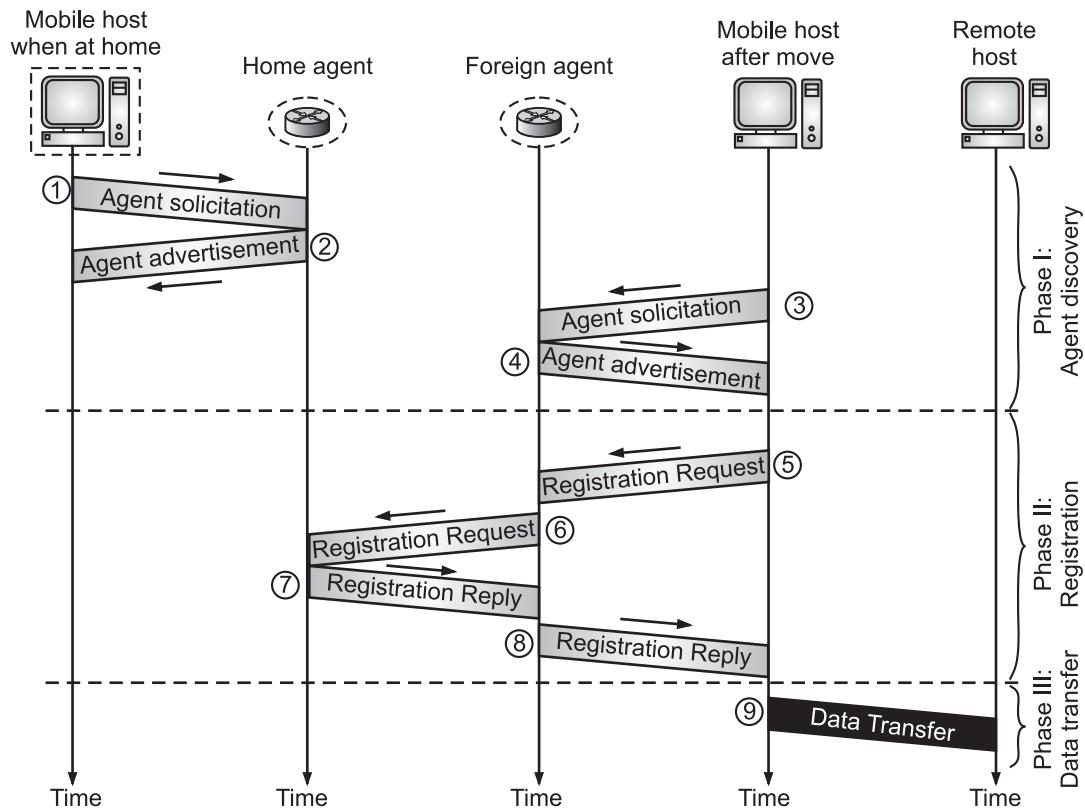


Fig. 3.45: Remote Host and Mobile Host Communication

Agent Advertisement:

- When a router advertises its presence on a network using an ICMP router advertisement, it can append an agent advertisement to the packet if it acts as an agent.
- Fig. 3.46 shows how an agent advertisement is piggybacking to the router advertisement packet.
- Mobile IP does not use a new packet type for agent advertisement, it uses the router advertisement packet of ICMP (Internet Control Message Protocol) and appends an agent advertisement message.
- The field descriptions of agent advertisement in Fig. 3.46 are as follows:
 - Type** (8-bit) field is set to 16.

2. **Length** (8-bit) field defines the total length of the extension message (not the length of the ICMP advertisement message).
3. **Sequence Number** (16-bit) field holds the message number. The recipient can use the sequence number to determine if a message is lost.
4. **Lifetime** field defines the number of seconds that the agent will accept requests. If the value is a string of 1s, the lifetime is infinite.
5. **Code** field is an 8-bit flag in which each bit is set (1) or unset (0). The meanings of the bits are shown in following table:

Bit	Meaning
0	Registration required. No collocated care of addresses.
1	Agent is busy and does not accept registration at this moment.
2	Agent acts as a Home Agent (HA).
3	Agent acts as a Foreign Agent (FA).
4	Agent uses minimal encapsulation.
5	Agent uses Generic Routing Encapsulation (GRE).
6	Agent supports header compression.
7	Unused (0).

6. **Care-of Addresses** field contains a list of addresses available for use as care of addresses. The mobile host can choose one of these addresses. The selection of this care-of address is announced in the registration request.

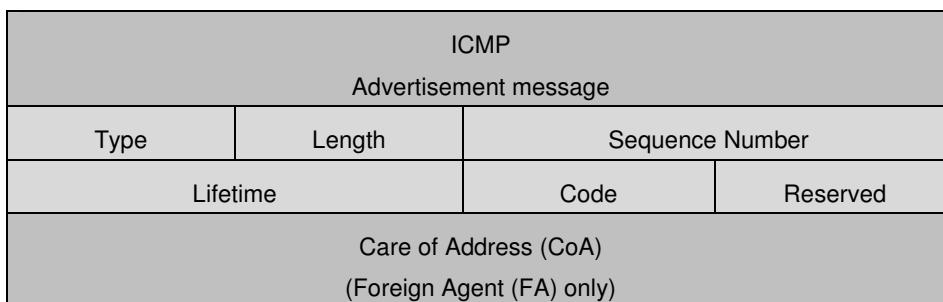


Fig. 3.46: Fields of Agent Advertisement

Agent Solicitation:

- When a mobile host has moved to a new network and has not received agent advertisements, it can initiate an agent solicitation by using the ICMP solicitation message to inform an agent that it needs assistance.

- Mobile IP does not use a new packet type for agent solicitation, it uses the router solicitation packet of ICMP.

Phase II: Registration:

- This is the second phase in the Mobile IP process, where a mobile node registers its current location with the foreign agent and the home agent.
- After a mobile host has moved to a foreign network and discovered the foreign agent, it must register.
- There are following four aspects of registration:
 - The mobile host must register itself with the foreign agent.
 - The mobile host must register itself with its home agent. This is normally done by the foreign agent on behalf of the mobile host.
 - The mobile host must renew registration if it has expired.
 - The mobile host must cancel its registration (deregistration) when it returns home.
- To register with the foreign agent and the home agent the mobile host uses a registration request and a registration reply as shown in Figs. 3.47 and 3.48.

Registration Request:

- A registration request is sent from the mobile host to the foreign agent to register its current address and also to announce its home address and home agent address.
- The foreign agent, after receiving and registering the request, relays the message to the home agent.
- Note that the home agent now knows the address of the foreign agent because the IP packet that is used for relaying has the IP address of the foreign agent as the source address.
- Fig. 3.47 shows the format of the registration request.

Type	Flag	Lifetime
Home address		
Home agent address		
Care of address		
Identification		
Extensions		

Fig. 3.47: Registration Request Format

- The field descriptions of registration request in Fig. 3.47 are as follows:
 - Type** (8-bit) field defines the type of the message. For a request message the value of this field is 1.
 - Flag** (8-bit) field defines forwarding information. The value of each bit have a meaning given in following table:

Bit	Meaning
0	Mobile host requests that home agent retain its prior care of address.
1	Mobile host requests that home agent tunnel any broadcast message.
2	Mobile host is using collocated care of addresses.
3	Mobile host requests that home agent use minimal encapsulation.
4	Mobile host requests Generic Routing Encapsulation (GRE).
5	Mobile host requests header compression.
6-7	Reserved bits.

- Lifetime** field defines the number of seconds the registration is valid. If the field is a string of 0s, the request message is asking for deregistration. If the field is a string of 1s, the lifetime is infinite.
- Home Address** field contains the permanent (first) address of the mobile host.
- Home Agent Address** contains the address of the home agent.
- Care of Address** field is temporary (second) address of the mobile host.
- Identification** field contains a 64-bit number that is inserted into the request by the mobile host and repeated in the reply message. It matches a request with a reply.
- Extensions** field used for authentication. Variable length extensions allow a home agent to authenticate the mobile agent.

Registration Reply:

- A registration reply is sent from the home agent to the foreign agent and then relayed to the mobile host.
- The reply confirms or denies the registration request. Fig. 3.48 shows the format of the registration reply.

Type	Code	Lifetime
Home address		
Home agent address		
Identification		
Extensions		

Fig. 3.48: Registration Reply Format

- The fields are similar to those of the registration request with the exceptions like the value of the type field is 3, the code field replaces the flag field and shows the result of the registration request (acceptance or denial). and the care-of address field is not needed.
- Registration messages are encapsulated in a UDP user datagram. An agent uses the well-known port 434; a mobile host uses an ephemeral port.

Phase III: Data Transfer:

- After agent discovery and registration, a mobile host can communicate with a remote host.
- Fig. 3.49 shows the communication idea.

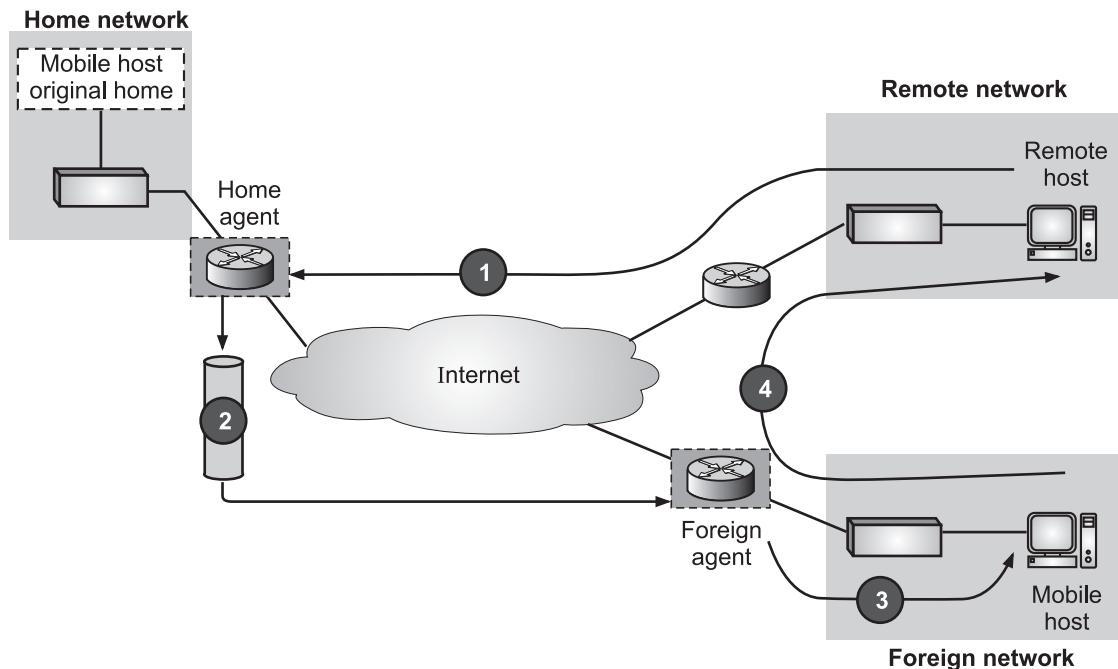


Fig. 3.49: Data Transfer Phase in Mobile IP

From Remote Host to Home Agent:

- When a remote host wants to send a packet to the mobile host, it uses its address as the source address and the home address of the mobile host as the destination address.
- In other words, the remote host sends a packet as though the mobile host is at its home network.
- The packet, however, is intercepted by the home agent, which pretends it is the mobile host. This is done using the proxy ARP technique.
- Path 1 of Fig. 3.49 shows this step.

From Home Agent to Foreign Agent:

- After receiving the packet, the home agent sends the packet to the foreign agent using the tunneling.
- The home agent encapsulates the whole IP packet inside another IP packet using its address as the source and the foreign agent's address as the destination.
- Path 2 of Fig. 3.49 shows this step.

From Foreign Agent to Mobile Host:

- When the foreign agent receives the packet, it removes the original packet.
- However, since the destination address is the home address of the mobile host, the foreign agent consults a registry table to find the address of the mobile host, (otherwise, the packet would just be sent back to the home network).
- The packet is then sent to the care of address. Path 3 of Fig. 3.49 shows this step.

From Mobile Host to Remote Host:

- When a mobile host wants to send a packet to a remote host (for example, a response to the packet it has received), it sends as it does normally.
- The mobile host prepares a packet with its home address as the source, and the address of the remote host as the destination.
- Although the packet comes from the foreign network, it has the home address of the mobile host.
- Path 4 of Fig. 3.49 shows this step.

3.7 NEXT GENERATION IP

- The network layer protocol in the TCP/IP protocol suite is currently IPv4 (Internetworking Protocol version 4).
- IPv4 has some deficiencies (like inefficient address space (32-bits), inefficient for audio and video data, no encryption and authentication security facility etc.) that make it unsuitable for the fast-growing Internet.
- To overcome these deficiencies IPv6 (Internetworking Protocol version 6) was proposed and is now a standard. IPv6 is the specific protocol chosen by the IETF (Internet Engineering Task Force) as the Internet's Next Generation IP.
- IPv6 is also called IPng (Internetworking Protocol, Next Generation). It has a 128-bit address space. IPv6 also includes addressing and security features.
- The next generation IP 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 32 bits).

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 packets. 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 novice users 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.

3.7.1 IPv6 Address Representation

- An IPv6 address consists of 16 bytes (octets); it is 128 bits long, as shown in Fig. 3.50.

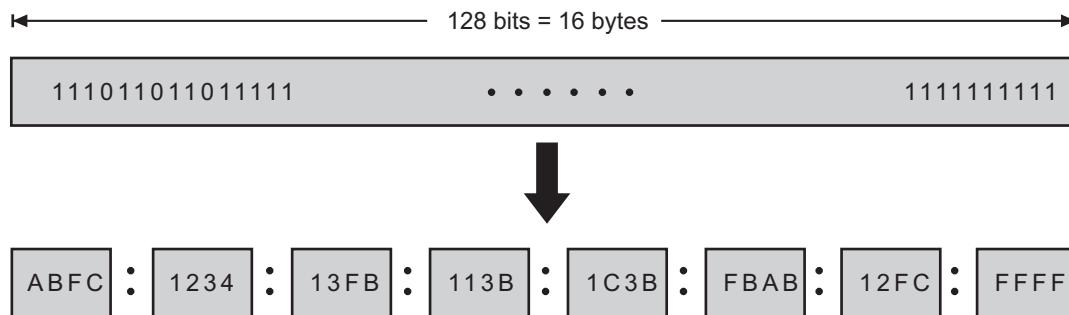


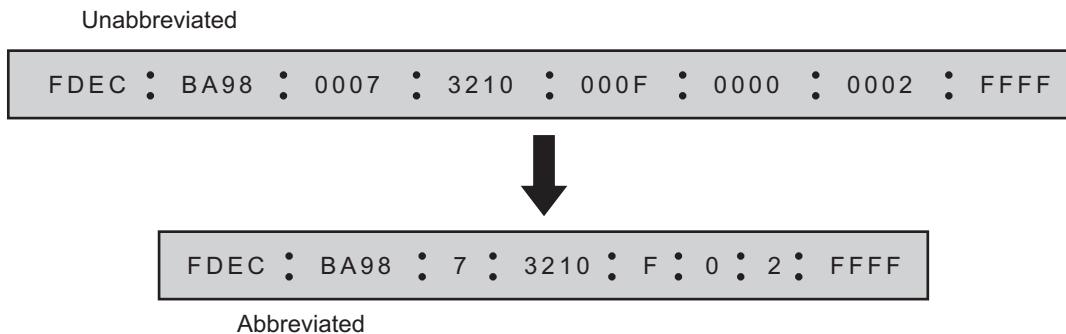
Fig. 3.50: IPv6 Address

Hexadecimal Colon Notation:

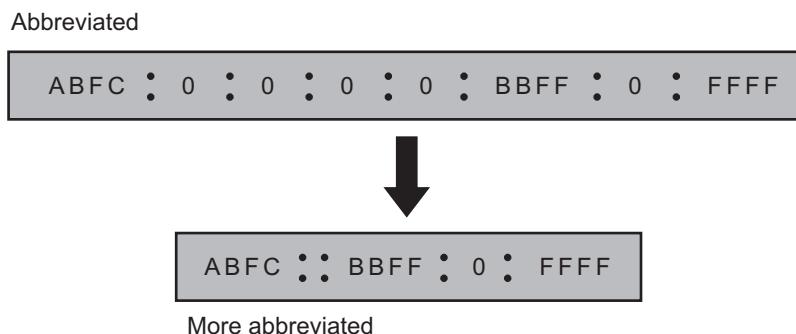
- To make addresses more readable, IPv6 specifies hexadecimal colon notation. In this notation, 128 bits are divided into eight sections, each of 2 bytes in length.
- Two bytes in hexadecimal notation require four hexadecimal digits. Therefore, the address consists of 32 hexadecimal digits, with every 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. 3.51).

**Fig. 3.51: Abbreviated Address**

- Using this form of abbreviation, 0007 can be written as 7, 000F as F, and 0000 as 0. Note that 3210 cannot 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 semicolons. Refer to the following Fig. 3.52. 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. 3.52: 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.

3.7.2 IPv6 Address Space

- The address space of IPv6 is much larger as compared to IPv4.

- The address space of IPv6 contains 2^{128} addresses as shown below and this address space is 2^{96} times of the IPv4 address,

340,282,366,920,938,463,374,607,431,768,211,456

3.7.3 IPv6 Address Types

- The addressing architecture of IPv6 is defined in RFC 4291 and allows three different types of transmission namely, unicast, anycast and multicast.

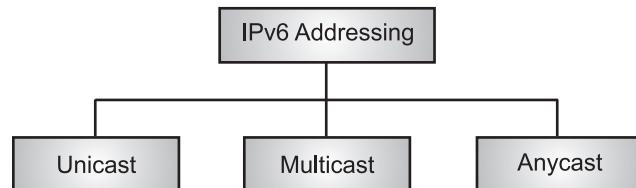


Fig. 3.53: Types of IPv6 Addressing

1. Unicast Address:

- A unicast address defines a single computer or router.
- The packet sent to the unicast address must be delivered to that specific/intended computer.

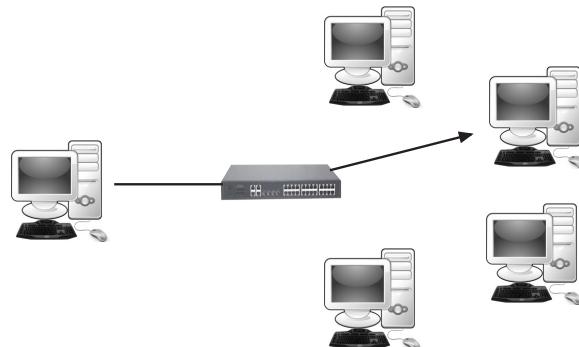


Fig. 3.54: Unicast Addressing

- IPv6 defines two types of unicast addresses namely, 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 Address:

- An anycast address is assigned to multiple interfaces (usually on multiple nodes). An anycast address defines a group of computers that all share a single 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.

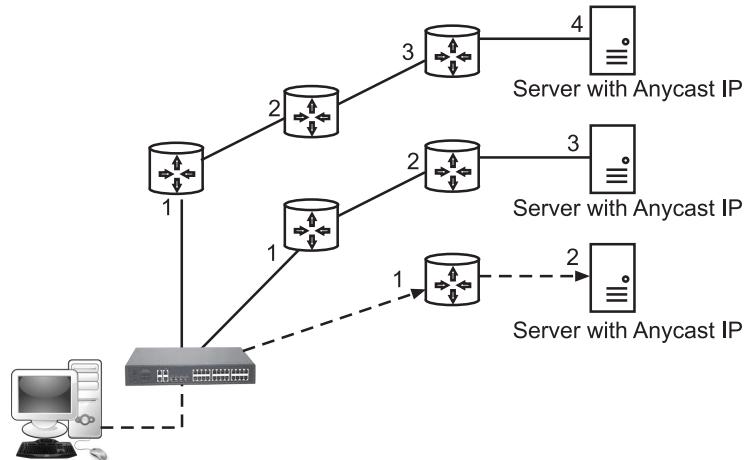


Fig. 3.55: Anycast Addressing

3. Multicast Address:

- It defines a group of computers. In multicast address each member of the group receives a copy.
- The packet sent to a multicast address must be delivered to each member of the group.

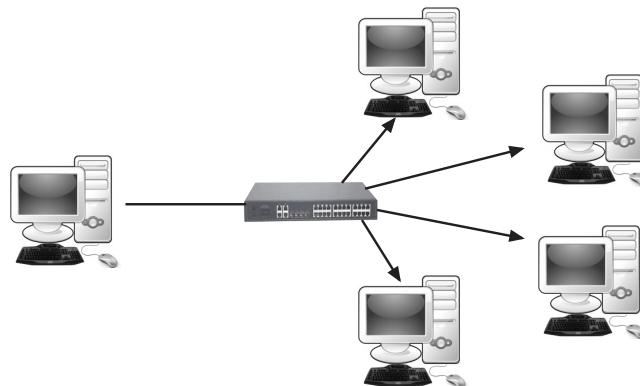


Fig. 3.56: Multicast Addressing

3.7.4 IPv6 Protocol

- Internet Protocol version 6 (IPv6) is a network layer protocol that enables data communications over a packet switched network.
- IPv6 is also called IPng (Internetworking Protocol next generation).
- Like IPv4, IPv6 is a connectionless, unreliable datagram protocol that is primarily responsible for addressing and routing packets between hosts.
- 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.

Features of IPv6:

1. **Expanded Addressing Capabilities:** IPv6 increases the IP address size from 32 bits to 128 bits, to support more levels in the addressing hierarchy, a much greater number of addressable nodes, and simpler auto-configuration of addresses.
2. **Support for Resource Allocation:** In IPv6, the type-of-service field has been removed, but two new fields, traffic class and flow label have been added to enable the source to request special handling of the packet. This mechanism can be used to support traffic such as real-time audio and video.
3. **Support for More Security:** The encryption and authentication options in IPv6 provide confidentiality and integrity of the packet. IPv6 basic specification includes security in the form of packet encryption and source authentication
4. **Header Format Simplification:** Some IPv4 header fields have been dropped or made optional, in IPv6 to reduce the common-case processing cost of packet handling and to limit the bandwidth cost of the IPv6 header.
5. **New Options:** IPv6 has new options to allow for additional functionalities.
6. **Auto-configuration:** IPv6 basic specification includes address auto-configuration. So, even a novice user can connect his/her machine to the Internet.
7. **Allowance for Extension:** IPv6 is designed to allow the extension of the protocol if required by new technologies or applications.
8. **Scalability:** IPv6 uses 128-bits address space and this address length is 4 times longer than IPv4 (32 bits). Thus many more IP addresses can be added to the Internet.
9. **Mobility:** IPv6 was designed keeping mobility in mind. This feature enables hosts, (such as mobile phones) to roam around in different geographical areas and remain connected with the same IP address. The mobility feature of IPv6 takes advantage of auto IP configuration and Extension headers.
10. **End to End Connectivity:** Every system now has a unique IP address and can traverse through the Internet without using NAT or other translating components. After IPv6 is fully implemented, every host can directly reach other hosts on the Internet, with some limitations involved like Firewall, organization policies, etc.

3.7.5 IPv6 Packet Format

- Fig. 3.57 shows the datagram/packet format of IPv6 protocol. Each packet in IPv6 consists of a mandatory base header followed by the payload.
- The payload includes two parts namely, optional extension headers and data from an upper layer.
- The base header consumes 40 bytes, inversely the extension headers and data from the top layer usually hold up to 65,535 bytes of information.

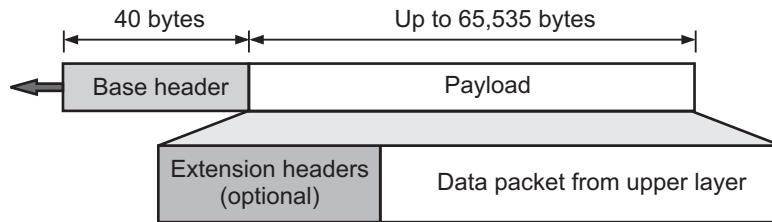


Fig. 3.57: IPv6 Datagram/Packet Format

Base Header:

- Fig. 3.58 shows the base header with its eight fields of IPv6 datagram.

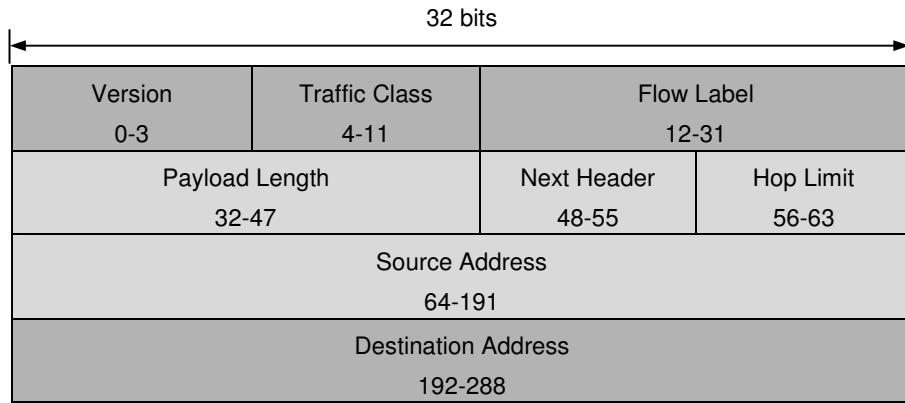


Fig. 3.58: Base Header Format of IPv6

- The various fields in IPv6 base header format are explained below:
 - Version** (4 bits) field specifies the version of Internet Protocol number. For IPv6 it is 6 i.e. 0110.
 - Traffic Class** (4 bits) field defines the priority of the packet with respect to traffic congestion.
 - Flow Label** (20 bits) field that is designed to provide special handling for a particular flow of data. The purpose of flow label field is to indicate that the packet belongs to a specific sequence of packets between source to destination and can be used to prioritized delivery of packets for services like voice.
 - Payload Length** (16 bits) is a field defining the total length of IP datagram including the base header.
 - Next Header** (8 bits) field identifies the type of header immediately following the IPv6 header.
 - Hop Limit** (8 bits) field serves the same purpose as the TTL (Time To Live) field in IPv4. The Hop Limit field shows the maximum number of routers the IPv6 packet can travel.

7. **Source Address** (128 bits) field identifies the original source of the datagram.
8. **Destination Address** (128 bits) field identifies the destination of the datagram.

3.7.6 Extension Header

- In IPv6, the fixed header contains only that much information which is necessary, avoiding that information which is either not required or is rarely used.
- All such information is put between the fixed header and the Upper layer header in the form of extension headers. Each extension header is identified by a distinct value.
- Extension headers allow additional functionality to be implemented in an IPv6 packet. These fields are used only for specific purposes. This permits the IPv6 packet to remain small and streamlined and possess only the fields that are required for its particular purpose.
- Fig. 3.59 shows the extension header format.

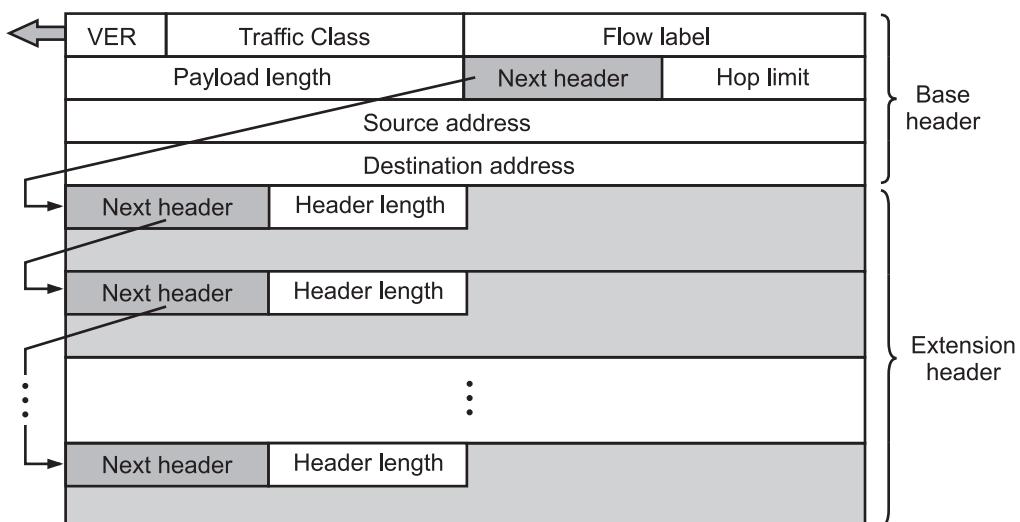


Fig. 3.59: Extension Header Format of IPv6

- When Extension Headers are used, IPv6 Fixed Header's Next Header field points to the first Extension Header. If there is one more Extension Header, then the first Extension Header's 'Next-Header' field points to the second one, and so on.
- The last Extension Header's 'Next-Header' field points to the Upper Layer Header. Thus, all the headers point to the next one in a linked list manner.
- If the Next Header field contains the value 59, it indicates that there are no headers after this header, not even Upper Layer Header.
- Each extension header is identified by a specific Next Header value, and the most common values are given in Table 3.5.

- IPv6 extension headers are optional but, when used, have specific ordering requirements that must be followed. This prevents the destination node from scanning the packet and looking for a particular type of extension header so that header can be processed ahead of the others.

Table 3.5: Extension Headers must be supported as per RFC

Sr. No.	Extension Header	Next Header Value	Description
1.	Hop-by-Hop options header	0	Read by all devices in the transit network.
2.	Routing header	43	Contains methods to support making routing decisions.
3.	Fragment header	44	Contains parameters of datagram fragmentation.
4.	Destination Options header	60	Read by destination devices.
5.	Authentication header	51	Information regarding authenticity.
6.	Encapsulating Security Payload (ESP) header	50	Encryption information.

- The sequence of Extension Headers should be:

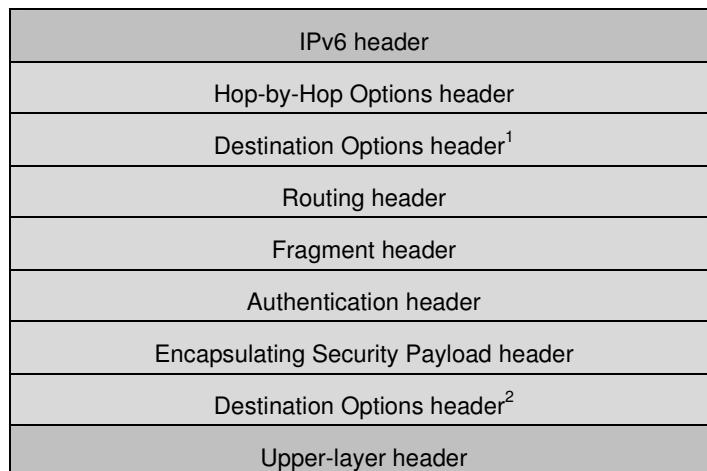


Fig. 3.60

- These headers:
 - should be processed by First and subsequent destinations.
 - should be processed by Final Destination.

- Extension Headers are arranged one after another in a linked list manner, as depicted in the Fig. 3.61.

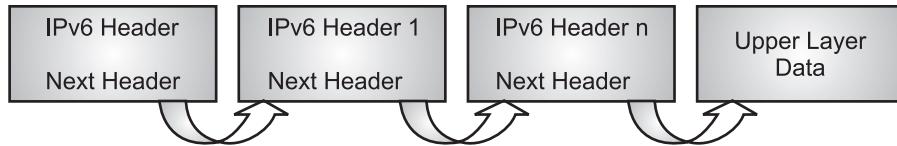


Fig. 3.61

3.7.7 Difference Between IPv4 and IPv6

- Following table differentiate between IPv4 and IPv6:

Sr. No.	IPv4	IPv6
1.	In IPv4 source and destination addresses are 32 bits (4 bytes) in length.	In IPv6 source and destination addresses are 128 bits (16 bytes) in length.
2.	IPv4 header is 20 bytes.	IPv6 header is 40 bytes.
3.	There are a maximum 2^{32} IP addresses.	There are maximum 2^{128} IP addresses.
4.	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:ABDB:BBCC:1234
5.	Checksum available in IPv4 header.	No Checksum field in IPv6 header.
6.	In IPv4 manual configuration is required or need to use DHCP.	IPv6 address can be configured automatically.
7.	In IPv4 the sending host and the router do the fragmentation.	In IPv6 only sending hosts do the fragmentation.
8.	IPv4 is being used as less secure protocol as its security section is dependent on application.	IPv6 has its inbuilt security feature named IPSec (Internet Protocol Security).
9.	IPv4 does not provide packet flow identification.	IPv6 packet flow identification is available within the IPv6 header using the Flow Label field.
10.	IPv4 does not provide encryption and authentication.	IPv6 provides encryption and authentication.
11.	IPv4 uses unicast, broadcast and multicast addresses.	IPv6 uses unicast, multicast and anycast addresses.

3.8 ROUTING

(April 18)

- When a network device has multiple paths to reach a destination, it always selects one path by preferring it over others. This selection process is termed as Routing.
- Routing is done by special network devices called routers or it can be done by means of software processes.
- Routing is the process of establishing the routes that data packets must follow to reach the destination.

3.8.1 General Idea of Routing

(April 18)

- Routing is a process of selecting the path along which the data can be transferred from source to the destination. Routing is performed by a special device known as a router.
- Routing is a process which is performed by layer 3 (network layer) devices in order to deliver the packet by choosing an optimal path from one network to another.
- In internetworking, routing is the process of moving a packet of data from source to destination.
- Routing is an activity that transmits information from a source address to a destination address through an interconnected network.
- When a router receives an IP packet, the router searches its routing table for the best matching route based on the destination IP address of the packet and forwards the packet through the outbound interface or next-hop IP address for the route.
- The routing table contains the routing entries (routes) learned by the router in various ways. The router can obtain routing entries in static or dynamic mode and maintain its own routing table.

Role of Router:

- A router selects routes and forwards packets. Upon receiving a packet, a router selects a proper path, which may have one or multiple hops, to send the packet to the next router according to the destination address in the packet. The last router is responsible for sending the packet to the destination host.
- A route is a path along which packets are sent from the source to the destination. When multiple routes are available to send packets from a router to the destination, the router can select the optimal route from an IP routing table.
- There are following three types of routing:
 1. **Static routing** is a process in which we have to manually add routes in the routing table.
 2. **Dynamic routing** makes automatic adjustment of the routes according to the current state of the route in the routing table.

3. **Default routing** is the method where the router is configured to send all packets towards a single router (next hop). It doesn't matter to which network the packet belongs, it is forwarded out to the router which is configured for default routing.

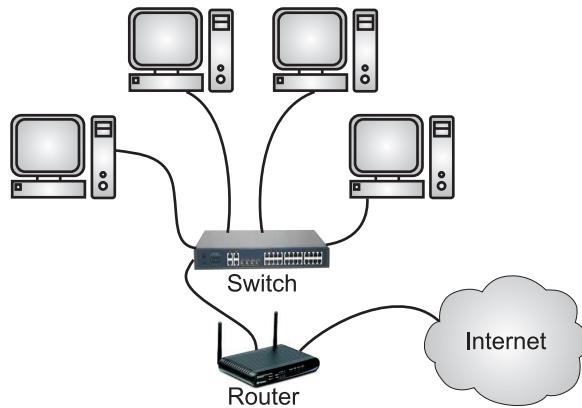


Fig. 3.62: Concept of Router

3.8.2 Routing Algorithms

- The routing algorithms are used for routing the packets. The routing algorithm is nothing but a software responsible for deciding the optimal path through which packets can be transmitted.
- A routing algorithm is a set of step-by-step operations used to direct Internet traffic efficiently.
- When a packet of data leaves its source, there are many different paths it can take to its destination. The routing algorithm is used to determine/choose the best path from source to destination. Different routing algorithms use different methods to determine the best path.
- Routing is the process of establishing the routes that data packets must follow to reach the destination.
- A routing algorithm specifies how packets choose the path to their destinations. There are two types of routing algorithms namely, deterministic and adaptive.
- In deterministic routing only one path is determined through source to destination, while adaptive routing algorithms allow multiple paths.
- The main properties of routing are:
 - 1. **Correctness:** The routing should be done properly and correctly so that the packets may reach their proper destination.
 - 2. **Simplicity:** The routing should be done in a simple manner so that the overhead is as low as possible. With increasing complexity of the routing algorithms the overhead also increases.

(April 18)

- 3. **Robustness:** Once, a major network becomes operative, it may be expected to run continuously for years without any failures. The algorithms designed for routing should be robust enough to handle hardware and software failures and should be able to cope with changes in the topology and traffic without requiring all jobs in all hosts to be aborted and the network rebooted every time some router goes down.
- 4. **Stability:** The routing algorithms should be stable under all possible circumstances.
- 5. **Fairness:** Every node connected to the network should get a fair chance of transmitting their packets. This is generally done on a first come first serve basis.
- 6. **Optimality:** The routing algorithms should be optimal in terms of throughput and minimizing mean packet delays. Here there is a trade-off and one has to choose depending on his suitability.
- The routing algorithm can be classified into following two types:
 1. **Static (Non-Adaptive) Routing Algorithms:**
 - In this type of algorithm, the network topology determines the final path. All the possible paths which are already calculated are loaded into the routing table.
 - Static routing is suitable for small networks. The disadvantage of static routing is, inability to respond quickly in case of network failure.
 2. **Dynamic (Adaptive) Routing Algorithms:**
 - The dynamic routing algorithm can change their routing decision on the basis of some changes made in the topology.
 - Each router can check the network status by communicating with the neighbors. So, the changes in the topology are reflected to all routers.
 - Finally, the router can calculate the suitable path to the final destination. The disadvantage of this type is its complexity in the router.

3.8.3 Types of Routing Algorithms

- In this section we will study various routing algorithms like distance vector routing algorithm, link state routing algorithm and path-vector routing algorithm.

3.8.3.1 Distance Vector Routing Algorithm

- Distance vector routing algorithm is the dynamic routing algorithm in computer networks. Distance vector routing algorithm also known as Bellman-Ford routing algorithm (also called Ford-Fulkerson algorithm) to find the shortest path between nodes in a graph given the distance between nodes.
- It was designed for small network topologies. Distance Vector Routing (DVR) method sees an AS, with all routers and networks, as a graph, a set of nodes and lines (edges) connecting the nodes.

- A router can normally be represented by a node and a network by a link connecting two nodes, although other representations are also possible.
- In the distance vector routing algorithm, the node router constructs a table containing the distance (total cost of path) to all other nodes and distributes that vector to its immediate neighbors.
- For distance vector routing, it is assumed that each node knows the cost of the link to each of its directly connected neighbors.
- A link, which is 'down' (which is not working) is assigned as an infinite cost. Every node sends a message to its directly connected neighbors.
- For example: A sends its information to B and F.
- After communicating to each directly connected node the shortest path can be easily computed (See Fig. 3.63).

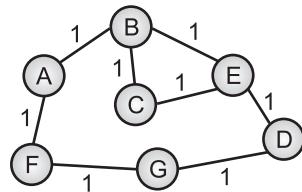


Fig. 3.63: Distance Vector Routing

- The shortest path can be computed as:

Information at Node	Cost to Reach Node						
	A	B	C	D	E	F	G
A	0	1	2	3	2	1	2
B	1	0	1	2	1	2	3
C	2	1	0	2	1	3	3
D	3	2	2	0	1	2	2
E	2	1	1	1	0	3	2
F	1	2	3	2	3	0	1
G	2	3	3	1	2	1	0

- Distance vector routing protocols are like road signs because routers must make preferred path decisions based on a distance or metric to a network.
- Just as travelers trust a road sign to accurately state the distance to the next town, a distance vector router trusts that another router is advertising the true distance to the destination network.

- In distance vector routing, the least-cost route between any two nodes is the route with minimum distance (m_i). In this protocol, as the name implies, each node maintains a vector (table) of minimum distances to every node.
- The table at each node also guides the packets to the desired node by showing the next stop in the route (next-hop routing).

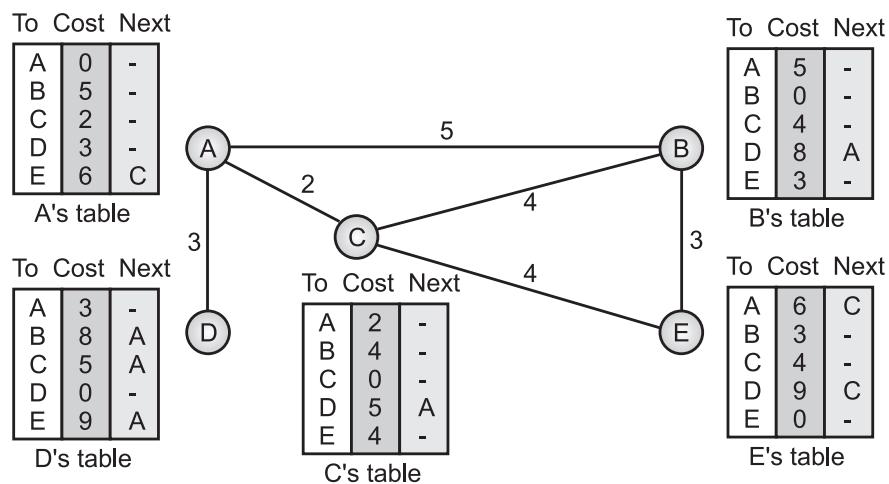


Fig. 3.64: Distance Vector Routing Tables

- The table for node A in Fig. 3.64 shows how we can reach any node from this node. For example, our least cost to reach node E is 6. The route passes through C.
- **Initialization:** The tables in Fig. 3.64 are stable; each node knows how to reach any other node and the cost. At the beginning, however, this is not the case. Each node can know only the distance between itself and its immediate neighbors, those directly connected to it. So for the moment, we assume that each node can send a message to the immediate neighbors and find the distance between itself and these neighbors. The distance for any entry that is not a neighbor is marked as infinite (unreachable).
- **Sharing:** The whole idea of distance vector routing is the sharing of information between neighbors. Although node A does not know about node E, node C does. So if node C shares its routing table with A, node A can also know how to reach node E. On the other hand, node C does not know how to reach node D, but node A does. If node A shares its routing table with node C, node C also knows how to reach node D. In other words, nodes A and C, as immediate neighbors, can improve their routing tables if they help each other.

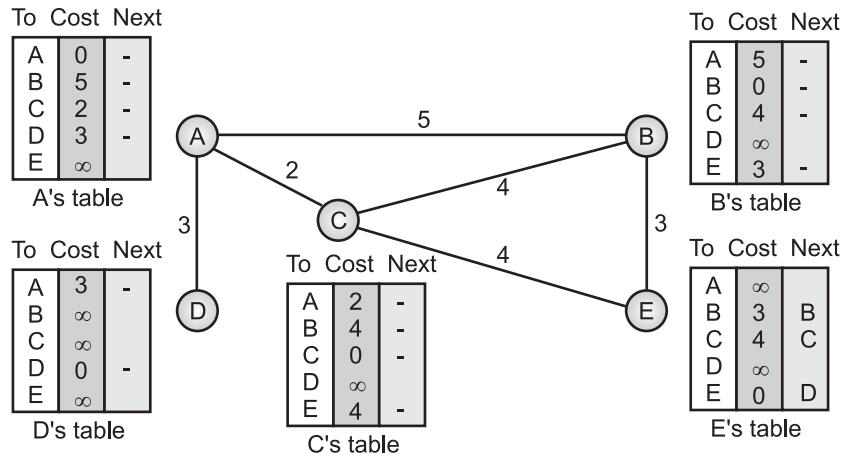


Fig. 3.65: Initialization of Tables in Distance Vector Routing (DVR)

- **Updating:** When a node receives a two-column table from a neighbor, it needs to update its routing table. Updating takes following three steps:

- Step 1:** The receiving node needs to add the cost between itself and the sending node to each value in the second column. The logic is clear. If node C claims that its distance to a destination is $x m_i$, and the distance between A and C is $y m_i$, then the distance between A and that destination, via C, is $x + y m_i$.
- Step 2:** The receiving node needs to add the name of the sending node to each row as the third column if the receiving node uses information from any row. The sending node is the next node in the route.
- Step 3:** The receiving node needs to compare each row of its old table with the corresponding row of the modified version of the received table.
- If the next-node entry is different, the receiving node chooses the row with the smaller cost. If there is a tie, the old one is kept.
 - If the next-node entry is the same, the receiving node chooses the new row. For example, suppose node C has previously advertised a route to node X with distance 3.

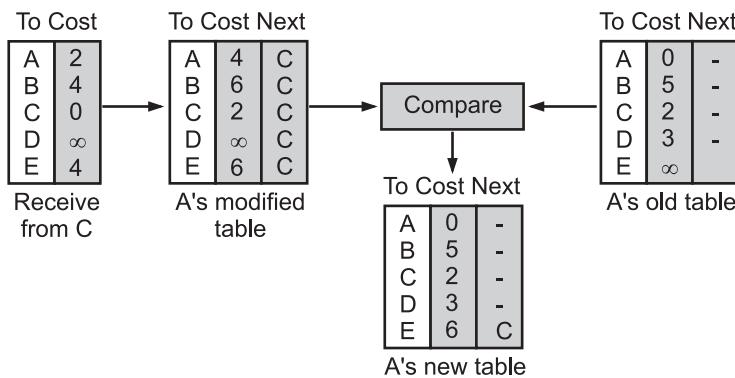


Fig. 3.66: Updating Distance Vector Routing

Bellman-Ford Algorithm:

- The Bellman–Ford algorithm is an algorithm that computes shortest paths from a single source vertex to all of the other vertices in a weighted digraph.
- Bellman-Ford algorithm solves single shortest path problem in which edge weight may be negative but no negative cycle exists.
- The Bellman–Ford algorithm works correctly when some of the edges of the directed graph G may have negative weight. When there are no cycles of negative weight, then we can find out the shortest path between source and destination.
- It is slower than Dijkstra's algorithm but more versatile, as it is capable of handling some of the negative weight edges. This algorithm detects the negative cycle in a graph and reports their existence.
- Based on the "Principle of Relaxation" in which more accurate values gradually recovered an approximation to the proper distance by until eventually reaching the optimum solution.
- Given a weighted directed graph $G = (V, E)$ with source s and weight function $w: E \rightarrow R$, the Bellman-Ford algorithm returns a Boolean value indicating whether or not there is a negative weight cycle that is attainable from the source.
- If there is such a cycle, the algorithm produces the shortest paths and their weights. The algorithm returns TRUE if and only if a graph contains no negative - weight cycles that are reachable from the source.

Recurrence Relation:

$\text{dist}_k[u] = [\min[\text{dist}_{k-1}[u], \min[i \in \text{edges}(u) : \text{dist}_{k-1}[i] + \text{cost}[i, u]]]$ as i except u .

$k \rightarrow k$ is the source vertex

$u \rightarrow u$ is the destination vertex

$i \rightarrow$ no of edges to be scanned concerning a vertex.

- Bellman-Ford algorithm can be used in many applications in graph theory. Given a graph and a source vertex src in the graph, find shortest paths from src to all vertices in the given graph.
- The graph may contain negative weight edges. Time complexity of this algorithm is $O(VE)$ which is more than Dijkstra's algorithm $O(V \log V)$ with the use of Fibonacci heap.

Input: Graph with source vertex src .

Output: Shortest distance to all vertices from src . If there is a negative weight cycle, then shortest distances are not calculated, negative weight cycle is reported.

Step 1: This step initializes distances from source to all vertices as infinite and distance to source itself is 0. Array $\text{dis}[]$ of size v will keep these values.

Step 2: This step calculates shortest distances. Do following $|V|-1$ times.

Do following for each edge $u-v$

If $\text{dist}[v] > \text{dist}[u] + \text{weight of } u-v$ then

$\text{dist}[v] = \text{dist}[u] + \text{weight of } u-v$

Step 3: This step reports if there is negative weight cycle in graph

Do the following for each edge $u-v$

If $\text{dist}[v] > \text{dist}[u] + \text{weight of edge } u-v$ then

“Graph contains negative weight cycle”

- The sequence of steps in Bellman-Ford algorithm are given below:

BELLMAN-FORD(G, w, s)

- INITIALIZE-SINGLE-SOURCE(G, s)
- for $i \leftarrow 1$ to $|V[G]| - 1$
- do for each edge $(u, v) \in E[G]$
- do RELAX(u, v, w)
- for each edge $(u, v) \in E[G]$
- do if $d[v] > d[u] + w(u, v)$
- then return FALSE
- return TRUE

Examples:

Example 1: Fig. 3.67 shows a map with nodes and lines and the cost of each line is given over the line. Find the least cost between the nodes.

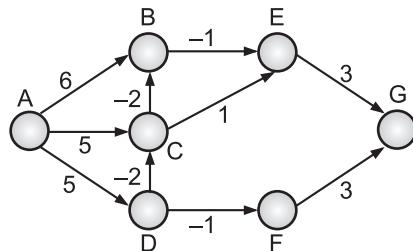


Fig. 3.67

Solution: List of edges: $(a, b), (a, c), (a, d), (b, e), (c, b), (c, e), (d, c), (d, f), (e, g), (f, g)$.

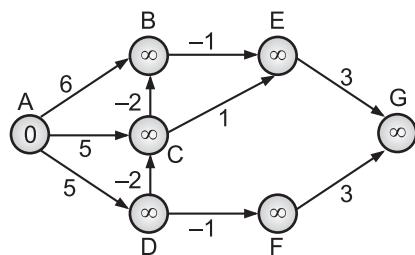


Fig. 3.68

Initially:

Node	A	B	C	D	E	F	G
Distance	0	∞	∞	∞	∞	∞	∞
Distance From							

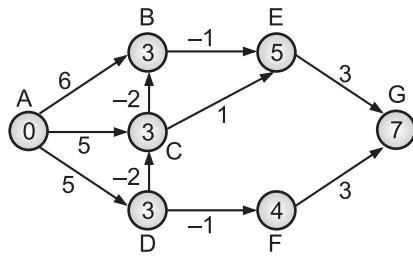


Fig. 3.69

Iteration 1:

Node	A	B	C	D	E	F	G
Distance	0	3	3	5	5	4	7
Distance From	0	C	D	A	B	D	F

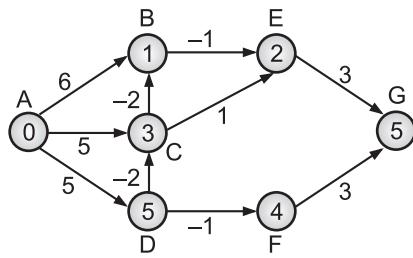


Fig. 3.70

Iteration 2:

Node	A	B	C	D	E	F	G
Distance	0	1	3	5	2	4	5
Distance From	0	C	D	A	B	D	E

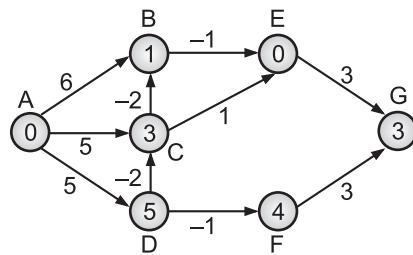


Fig. 3.71

Iteration 3:

Node	A	B	C	D	E	F	G
Distance	0	1	3	5	0	4	3
Distance From	0	C	D	A	B	D	E

Example 2: Fig. 3.72 shows a map with nodes and lines and the cost of each line is given over the line. Find the least cost between the nodes.

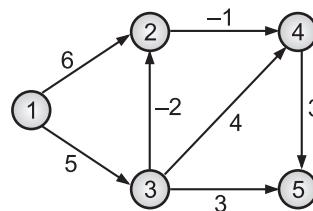


Fig. 3.72

Solution: Here, first we list all the edges and their weights.

	Vertices				
No. of edges traversed	1	2	3	4	5
1	0	6	5	∞	∞
2	0	3	5	5	8
3	0	3	5	2	8
4	0	3	5	2	5

Example 3: Fig. 3.73 shows a map with nodes and lines and the cost of each line is given over the line. Find the least cost between the nodes.

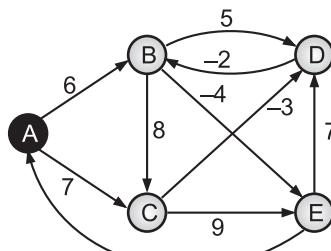
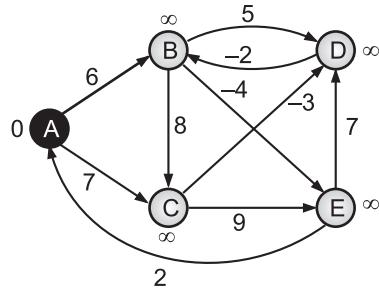


Fig. 3.73

Solution:

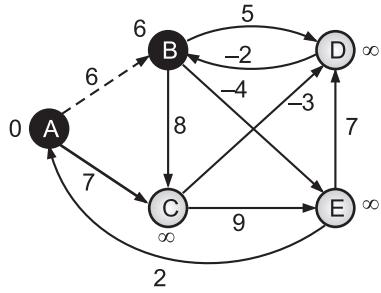
Step 1: Consider A as a source index.



No. of Nodes	A	B	C	D	E
Distance	0	6	7	∞	∞
Distance From	A	A	A		

Fig. 3.74

Step 2: Consider Vertex B.



No. of Nodes	A	B	C	D	E
Distance	0	6	7	11	2
Distance From	A	A	A	B	B

Fig. 3.75

Step 3: Consider Vertex E.

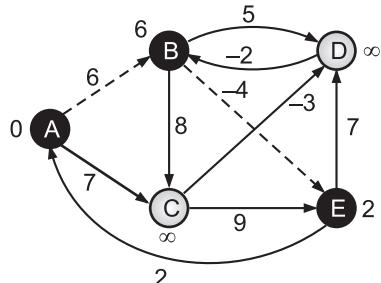


Fig. 3.76

No. of Nodes	A	B	C	D	E
Distance	0	6	7	9	2
Distance From	A	A	A	E	B

Step 4: Consider Vertex C.

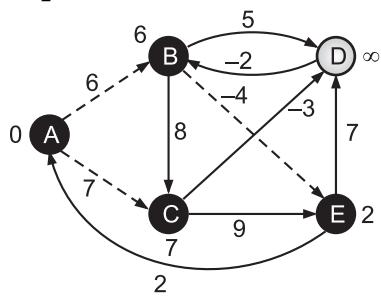


Fig. 3.77

No. of Nodes	A	B	C	D	E
Distance	0	6	7	4	2
Distance From	A	A	A	C	B

Step 5: Consider Vertex D.

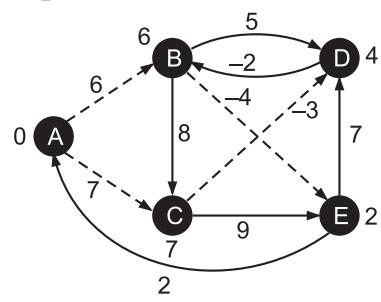


Fig. 3.78

No. of Nodes	A	B	C	D	E
Distance	0	2	7	4	2
Distance From	A	D	A	C	B

Step 6: Consider Vertex B.

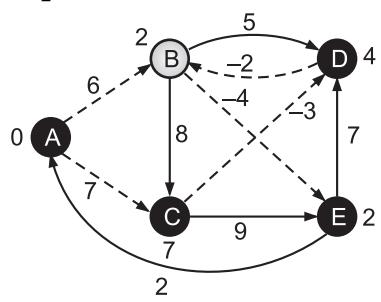
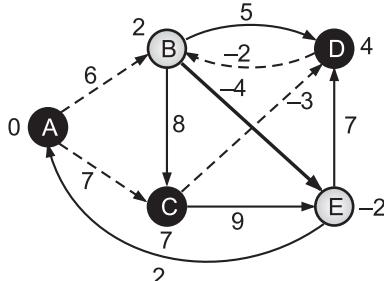


Fig. 3.79

No. of Nodes	A	B	C	D	E
Distance	0	2	7	4	-2
Distance From	A	D	A	C	B

Step 7: Consider Vertex E.



No. of Nodes	A	B	C	D	E
Distance	0	2	7	4	-2
Distance From	A	D	A	C	B

Fig. 3.80

Result:

Vertex	Distance From A
A	0
B	2
C	7
D	4
E	-2

3.8.3.2 Link State Routing Algorithm

- Link state routing is a technique in which each router shares the knowledge of its neighborhood with every other router in the internetwork.
- Link state routing has a different philosophy from that of distance vector routing.
- In link state routing, if each node in the domain has the entire topology of the domain the list of nodes and links, how they are connected including the type, cost (metric), and condition of the links (up or down)-the node can use Dijkstra's algorithm to build a routing table.
- Link state routing protocols are more like a road map because they create a topological map of the network and each router uses this map to determine the shortest path to each network.
- Just as you refer to a map to find the route to another town, link-state routers use a map to determine the preferred path to reach another destination.
- Routers running a link state routing protocol send information about the state of its links to other routers in the routing domain.
- The state of those links refers to its directly connected networks and includes information about the type of network and any neighboring routers on those networks-hence the name link state routing protocol.

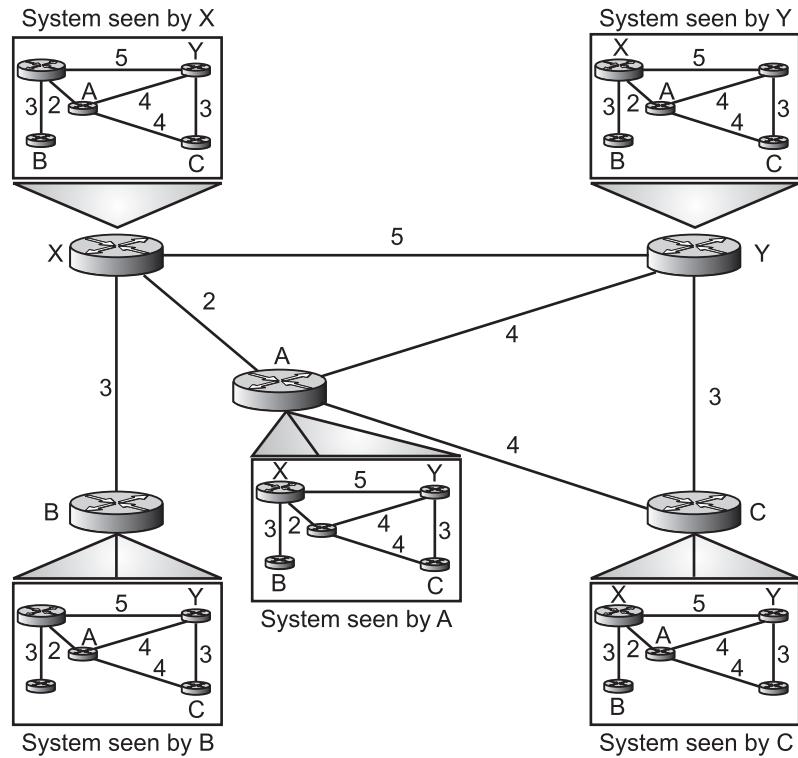


Fig. 3.81: Concept of Link State Routing (LSR)

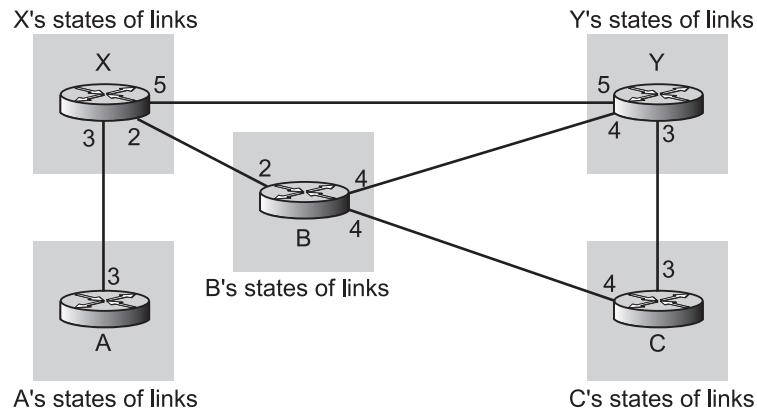


Fig. 3.82: Link State Knowledge

- The Fig. 3.82 shows a simple domain with five nodes. Each node uses the same topology to create a routing table, but the routing table for each node is unique because the calculations are based on different interpretations of the topology.
- This is analogous to a city map. While each person may have the same map, each needs to take a different route to reach her specific destination

Building Routing Tables:

- In link state routing, four sets of actions are required to ensure that each node has the routing table showing the least-cost node to every other node.
 1. Creation of the states of the links by each node, called the link state packet or LSP.
 2. Dissemination of LSPs to every other router, called flooding, in an efficient and reliable way.
 3. Formation of a shortest path tree for each node.
 4. Calculation of a routing table based on the shortest path tree.

Formation of Shortest Path Tree (Dijkstra Algorithm):

- A tree is a graph of nodes and links; one node is called the root. All other nodes can be reached from the root through only one single route.
- A shortest path tree is a tree in which the path between the root and every other node is the shortest. What we need for each node is a shortest path tree with that node as the root.
- The Dijkstra algorithm is used to create a shortest path tree from a given graph. The algorithm uses the following steps:
 - **Initialization:** Select the node as the root of the tree and add it to the path. Set the shortest distances for all the root's neighbors to the cost between the root and those neighbors. Set the shortest distance of the root to zero.
 - **Iteration:** Repeat the following two steps until all nodes are added to the path:
 1. **Adding the next node to the path:** Search the nodes not in the path. Select the one with minimum shortest distance and add it to the path.
 2. **Updating:** Update the shortest distance for all remaining nodes using the shortest distance of the node just moved to the path in Step 2.
 - $D_j = \min(D_j, D_i + c_{ij})$ for all remaining nodes.

Dijkstra Algorithm:

```

Dijkstra ()
{
// Initialization
Path = {s}           // s means self
for (i = 1 to N)
{
  If (i is a neighbor of s and I ≠ s) Di= csi
  if (i is not a neighbor of s)       Di=∞
}
Ds = 0

```

```

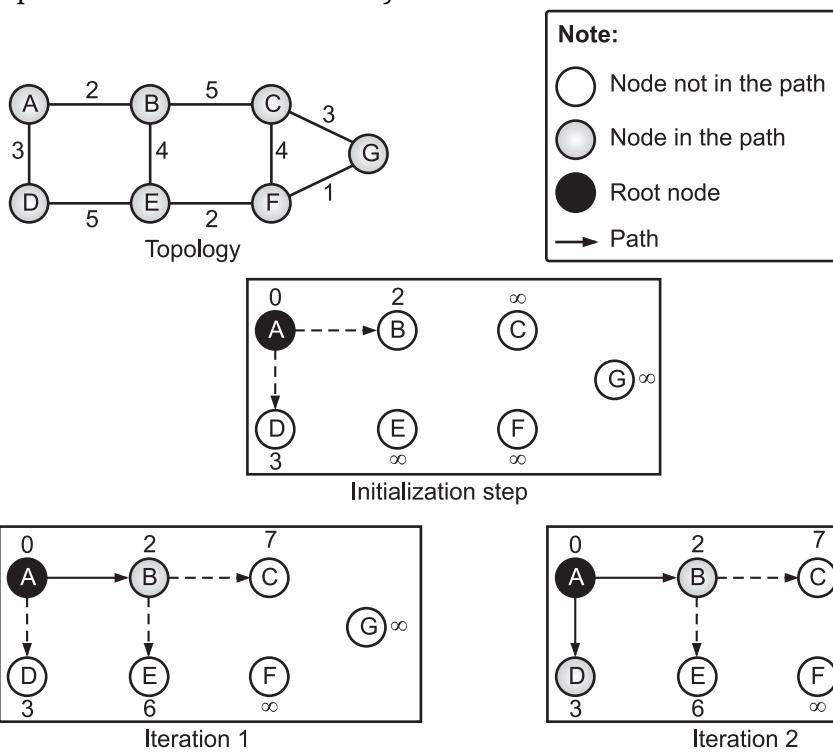
} // Dijkstra
// Iteration
Repeat
{
// Finding the next node to be added
Path = Path ∪ i if Di is minimum among all remaining nodes
// Update the shortest distance for the rest
for (j = 1 to M)           // M number of remaining nodes
{
Dj = minimum (Dj, Dj + cij)
}
} until (all nodes included in the path, M = 0)

```

Examples:

Example 1: Fig. 3.83 shows the formation of the shortest path tree for the graph of seven nodes.

In the initialization step, node A selects itself as the root. It then assigns shortest path distances to each node on the topology. The nodes that are not neighbors of A receive a shortest path distance value of infinity.



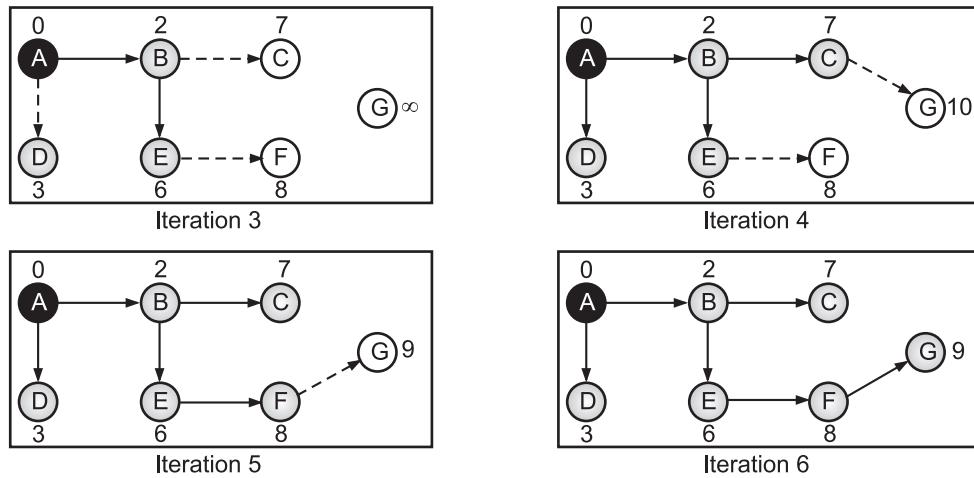


Fig. 3.83

Solution: In each iteration, the next node with minimum distance is selected and added to the path. Then all shortest distances are updated with respect to the last node selected. For example, in the first iteration, node B is selected and added to the path and the shortest distances are updated with respect to node B (The shortest distances for C and E are changed, but for the others remain the same). After six iterations, the shortest path tree is found for node A. Note that in iteration 4, the shortest path to G is found via C, but in iteration 5, a new shortest route is discovered (via G); the previous path is erased and the new one is added.

Calculation of Routing Table from Shortest Path Tree (SPT):

Each node uses the shortest path tree found in the previous discussion to construct its routing table. The routing table shows the cost of reaching each node from the root. Routing table for node A using the shortest path tree found in above Fig. 3.84.

Destination	Cost	Next Router
A	0	–
B	2	–
C	7	B
D	3	–
E	6	B
F	8	B
G	9	B

Fig. 3.84: Routing Table for Node A

Example 2: Consider Fig. 3.85. Find the shortest path.

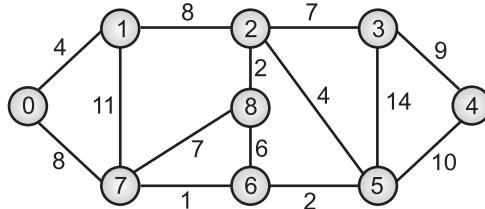


Fig. 3.85

Solution:

The set sptSet is initially empty and distances assigned to vertices are {0, INF, INF, INF, INF, INF, INF, INF, INF} where INF indicates infinite. Now pick the vertex with minimum distance value. The vertex 0 is picked, including it in sptSet. So sptSet becomes {0}. After including 0 to sptSet, update distance values of its adjacent vertices. Adjacent vertices of 0 are 1 and 7. The distance values of 1 and 7 are updated as 4 and 8. The vertices included in SPT are shown in black colour, (See Fig. 3.86).

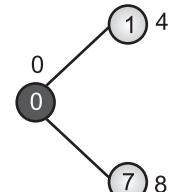


Fig. 3.86

Pick the vertex with minimum distance value and not already included in SPT (not in sptSET). The vertex 1 is picked and added to sptSet. So sptSet now becomes {0, 1}. Update the distance values of adjacent vertices of 1. The distance value of vertex 2 becomes 12, (See Fig. 3.87).

Pick the vertex with minimum distance value and not already included in SPT (not in sptSET). Vertex 7 is picked. So sptSet now becomes {0, 1, 7}. Update the distance values of adjacent vertices of 7. The distance value of vertex 6 and 8 becomes finite (15 and 9 respectively), (See Fig. 3.88).

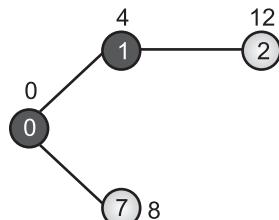


Fig. 3.87

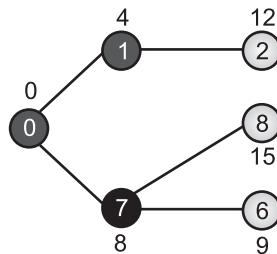


Fig. 3.88

Pick the vertex with minimum distance value and not already included in SPT (not in sptSET). Vertex 6 is picked. So sptSet now becomes {0, 1, 7, 6}. Update the distance values of adjacent vertices of 6, (See Fig. 3.89). The distance value of vertex 5 and 8 are updated.

We repeat the above steps until sptSet doesn't include all vertices of given graph. Finally, we get the Shortest Path Tree (SPT) as shown in Fig. 3.90.

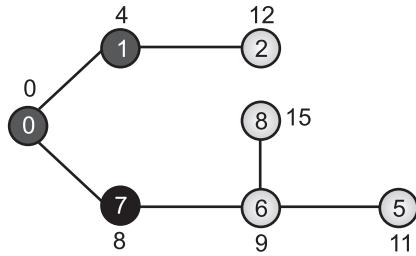


Fig. 3.89

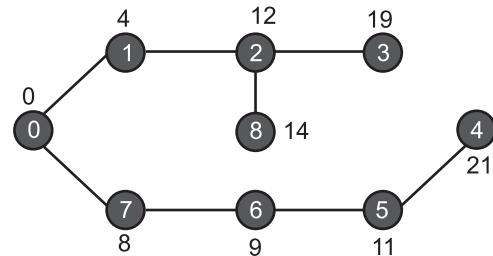


Fig. 3.90

Difference between Distance Vector Routing and Link State Routing:

Sr. No.	Distance Vector Routing	Link State Routing
1.	The distance vector routing determines the direction (vector) and distance (such as link cost or number of hops) to any link in the network.	The link state routing uses the Shortest Path First (SPF) algorithm to create an abstract of the exact topology of the entire network.
2.	Distance vector routing protocols do not have an actual map of the network topology.	A link state routing protocol is like having a complete map of the network topology.
3.	The distance vector routing algorithm is a type of routing algorithm that is based on the number of hops in a route between a source and destination computer.	The link state routing algorithm broadcasts information about the cost of reaching each of its neighbors to all other routers in the network.
4.	Uses Bellman-Ford algorithm.	Uses Dijkstra's algorithm.
5.	The name 'distance vector' is used because the routers exchange vectors containing distance and direction information.	In link state routing, each routing node makes a connectivity graph for the nodes in the network and independently calculates its shortest path to every other destination in the network.
6.	Less bandwidth is required.	High bandwidth is required.

Contd...

7.	Distance vector routing updates full routing table.	Link state routing updates only the link state.
8.	Example of distance vector routing protocols is RIP.	Example of link state routing protocols is OSPF.
9.	The utilization of CPU and memory in distance vector routing is lower than the link state routing.	Higher utilization of CPU and memory.
10.	Distance vector routing does not have any hierarchical design.	Link state routing works best for hierarchical routing design and in networks where fast convergence is crucial.

3.8.3.3 Path Vector Routing Algorithm

- A path vector routing is a more recent concept compared to both a distance vector routing and the link state routing.
- The path vector routing approach not only exchanges information about the existence of destination networks but also exchanges the path on how to reach the destination.
- Path information is used to determine the best paths and to prevent routing loops. The only widely used path vector protocol is BGP.
- Distance vector routing and link state routing are both intra-domain routing protocols. They can be used inside an autonomous system, but not between autonomous systems.
- These two protocols are not suitable for inter-domain routing mostly because of scalability. Both of these routing protocols become intractable when the domain of operation becomes large. Distance vector routing is subject to instability if there are more than a few hops in the domain of operation.
- Link state routing needs a huge amount of resources to calculate routing tables. It also creates heavy traffic because of flooding. There is a need for a third routing protocol which we call path vector routing.
- Path vector routing is used for inter-domain routing with low computational overhead and support of heterogeneous policies and securities advantages.
- Path vector routing proved to be useful for inter-domain routing. The principle of path vector routing is similar to that of distance vector routing.
- In path vector routing, we assume that there is one node in each autonomous system that acts on behalf of the entire autonomous system.

- **Initialization:** At the beginning, each speaker node can know only the reachability of nodes inside its autonomous system.

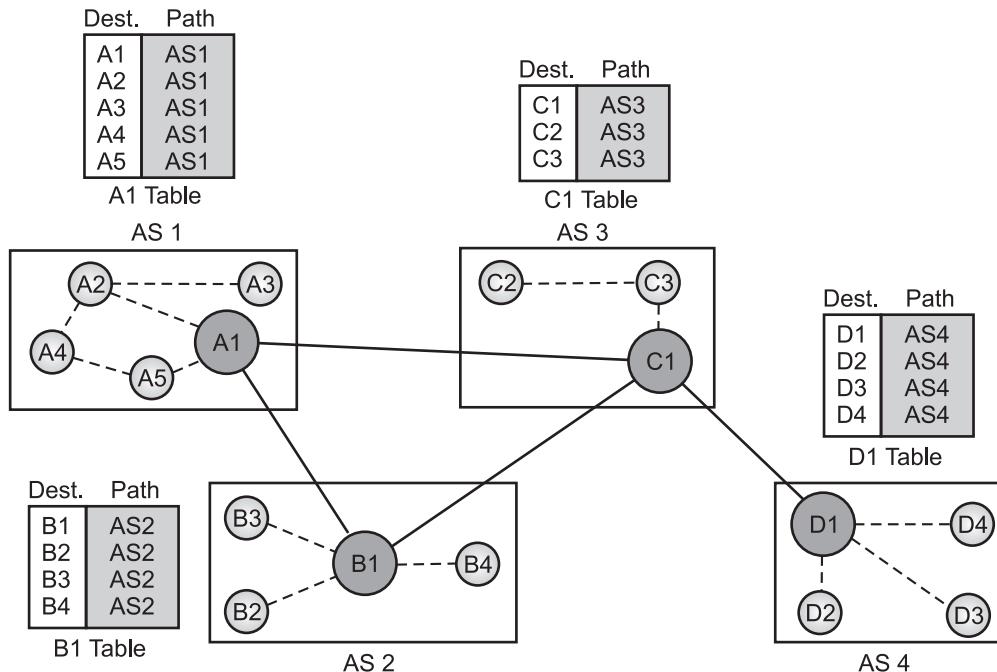


Fig. 3.91: Initial Routing Table in Path Vector Routing

- In Fig. 3.91, Node A1 is the speaker node for AS1, B1 for AS2, C1 for AS3, and D1 for AS4. Node A1 creates an initial table that shows A1 to A5 are located in AS1 and can be reached through it. Node B1 advertises that B1 to B4 are located in AS2 and can be reached through B1 and so on.
- A path vector protocol is a network routing protocol which maintains the path information that gets updated dynamically.
- Updates which have looped through the network and returned to the same node are easily detected and discarded. Border Gateway Protocol (BGP) is an example of a path vector protocol.

Disadvantages of Path Vector Routing:

1. **Lack of Congestion Control:** In path vector routing, the routing policies may be heterogeneous across the ASs. The network traffic or the link congestion may not be the criterion for path selection in the policies of any AS. Moreover, the path vector routing protocol converges very quickly and stabilizes. Thus, it may not be suitable for handling network congestion efficiently.
2. **Complex:** Path vector routing can be very complex to configure in the network.

3. **Load Balancing:** Load balancing between the source and destination can be done by disseminating packets through each of the alternative paths, multiple paths for packet dissemination are not selected to support load balancing.
4. **Inefficient Load Balancing:** The basic path vector routing protocol does not support load balancing. The path vector table may contain alternative paths to a destination, but an alternative path is selected generally on the failure of an existing path.

PRACTICE QUESTIONS

Q.I Multiple Choice Questions:

1. Which layer is responsible for the delivery of individual packets from the source to the destination host?

(a) Physical layer	(b) Network layer
(c) Data link layer	(d) Transport layer
2. Network layer services include _____.

(a) Routing and Forwarding	(b) Packetizing
(c) Flow and Error control	(d) All of these
3. Which is a situation in the network layer in which too many datagrams are present in an area of the Internet?

(a) Congestion	(b) Packetizing
(c) Flow and Error control	(d) All of these
4. The two congestion control mechanisms are _____.

(a) Open loop	(b) Closed loop
(c) Both (a) and (b)	(d) None of these
5. Which protocol is a set of rules that dictate how data should be delivered over the Internet

(a) IP	(b) UDP
(c) TCP	(d) All of these
6. Which is an address used to uniquely identify a device on an IP network?

(a) UDP	(b) IP
(c) TCP	(d) All of these
7. The parts of an IP are _____.

(a) Network ID	(b) Host ID
(c) Both (a) and (b)	(d) None of these
8. Which is a 32-bits IP address?

(a) IPv4	(b) IPv6
(c) Both (a) and (b)	(d) None of these

9. IPv4 addressing uses the concept of classes known as _____ addressing.
- (a) Classless
 - (b) Classful
 - (c) Both (a) and (b)
 - (d) None of these
10. In a class A address, the first bit of the first octet is always ‘_____’.
- (a) 0
 - (b) 10
 - (c) 110
 - (d) 1110
11. Which is a process that extracts the address of the physical network from an IP address.
- (a) Subnetting
 - (b) Supernetting
 - (c) Masking
 - (d) None of these
12. IP networks can be divided into smaller networks called _____.
- (a) Subnets
 - (b) Subnetworks
 - (c) Both (a) and (b)
 - (d) None of these
13. Which is a method for partitioning/dividing a classful IP network into smaller subnetworks (subnets)?
- (a) Subnetting
 - (b) Supernetting
 - (c) Masking
 - (d) None of these
14. Which is a logical partition of an IP network into multiple, smaller network segments?
- (a) Supernets
 - (b) Subnets
 - (c) Masks
 - (d) None of these
15. Which allows multiple networks to be specified by one subnet mask?
- (a) Subnetting
 - (b) Supernetting
 - (c) Masking
 - (d) None of these
16. Which is a technology that supports mobile data and applications that are dealing with wireless connectivity.
- (a) Mobile IP
 - (b) Masking IP
 - (c) Subnet IP
 - (d) None of these
17. Which stores information about mobile nodes visiting its network?
- (a) Home Agent (HA)
 - (b) Mobile Node (MN)
 - (c) Foreign Agent (FA)
 - (d) All of these
18. Which is a network to which the mobile node originally belongs to as per its assigned IP address (home address)?
- (a) Home network
 - (b) Mobile network
 - (c) Foreign network
 - (d) None of these

19. Which translates the IP addresses of computers in a local network to a single IP address?
- (a) Mask
 - (b) Supernet
 - (c) NAT
 - (d) None of these
20. A datagram is a variable length packet which contains two parts namely,
- (a) Header
 - (b) Data
 - (c) Both (a) and (b)
 - (d) None of these
21. The three phases of Mobile IP (MIP) includes,
- (a) agent discovery (involves the mobile host, the foreign agent and the home agent)
 - (b) registration (also involves the mobile host and the two agents)
 - (c) data transfer (remote host is also involved)
 - (d) All of these
22. Which is a network layer protocol that enables data communications over a packet switched network?
- (a) UDP
 - (b) IPv6
 - (c) TCP
 - (d) TCP/IP
23. Which headers allow additional functionality to be implemented in an IPv6 packet?
- (a) Forwarding
 - (b) Back wording
 - (c) Extension
 - (d) None of these
24. Which is the process of establishing the routes that data packets must follow to reach the destination?
- (a) Switching
 - (b) Routing
 - (c) Forwarding
 - (d) None of these
25. Which is used for routing the packets in routing?
- (a) Table
 - (b) NAT
 - (c) Algorithms
 - (d) None of these
26. Which routing algorithms do not base their routing decisions on measurements or estimates of the current traffic and topology?
- (a) Adaptive
 - (b) Non-adaptive
 - (c) Both (a) and (b)
 - (d) None of these
27. Which algorithms change their routing decisions to reflect changes in the topology, and usually the traffic as well.
- (a) Adaptive
 - (b) Non-adaptive
 - (c) Both (a) and (b)
 - (d) None of these

28. Which is a routing algorithm in which every router maintains a database with one entry for each possible destination on the network?

- | | |
|---------------------|-------------------|
| (a) Path Vector | (b) Link State |
| (c) Distance Vector | (d) None of these |

ANSWERS

1. (b)	2. (d)	3. (a)	4. (c)	5. (a)	6. (b)	7. (c)
8. (a)	9. (b)	10. (a)	11. (c)	12. (c)	13. (a)	14. (b)
15. (b)	16. (a)	17. (c)	18. (a)	19. (c)	20. (c)	21. (d)
22. (b)	23. (c)	24. (b)	25. (c)	26. (b)	27. (a)	28. (c)

Q. II Fill in the Blanks:

1. _____ layer is responsible for routing packets from the source host to the destination host.
2. _____ control in the network layer is the process of detecting and correcting data packets that have been corrupted or lost during transmission.
3. The network layer receives the data from the upper layers and creates its own packets by encapsulating these packets. The process is known as _____.
4. _____ control refers to the techniques used to control or prevent congestion.
5. Congestion control refers to techniques and mechanisms that can either prevent congestion, before it _____, or remove congestion, after it has _____.
6. The Internet Protocol Address (IP Address) is a unique _____ assigned to every computing device, such as personal computers, tablets, and smartphones use to identify itself and communicate with other devices in the IP network.
7. _____ is responsible for packetizing, forwarding and delivery of a packet at the network layer.
8. Dividing a large block of addresses into several contiguous sub-blocks and assigning these sub-blocks to different smaller networks is called _____.
9. In _____ addressing, the address space is divided into five classes namely, A, B, C, D and E.
10. A _____ mask (or number) is used to determine the number of bits used for the subnet and host portions of the address.
11. When IP is used as a connection less protocol, _____ is based on the destination address of the IP datagram when the IP is used as a connection oriented protocol, forwarding is based on the label attached to an IP datagram.
12. Internet Protocol is _____ and unreliable protocol.

13. Packets in the network (internet) layer are called ____.
14. IPv6 addresses have ____ bits.
15. ____ address in IPv6 identifies a single network interface.
16. A ____ is a networking device that forwards data packets between computer networks. (#ing)
17. Routers perform the traffic directing functions on the ____.
18. A subnet is a ____ partition of an IP network into multiple, smaller network segments.
19. A routing ____ is a method for determining the routing of packets in a node. For each node of a network, the algorithm determines a routing table, which in each destination, matches an output line.
20. ____ vector routing algorithms require that each node exchanges information between neighbors, that is to say between nodes directly connected.
21. A routing ____ is a grouping of information stored on a networked computer or network router that includes a list of routes to various network destinations.
22. The ____ state routing algorithm is used to find the shortest path from one node to every other node in the network.
23. In ____ addressing, there are no classes, but the addresses are still granted in blocks.

ANSWERS

1. Network	2. Error	3. packetizing	4. Congestion
5. happens, happened	6. number	7. IPv4	8. subnetting
9. classful	10. subnet	11. forwarding	12. connectionless
13. datagrams	14. 128	15. Unicast	16. router
17. Internet	18. logical	19. algorithm	20. Distance
21. table	22. link	23. classless	

Q. III State True or False:

1. With the help of forwarding, data packets are transferred from one place to another in the network.
2. Error occurs when the number of datagrams sent by source is beyond the capacity of the network.
3. Congestion control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened.

4. Open loop congestion control policies are applied to prevent congestion after it happens.
5. In general, we can divide congestion control mechanisms into two broad categories namely, open-loop congestion control (prevention) and closed-loop congestion control (removal).
6. Backpressure is a node-to-node congestion control technique that propagate in the opposite direction of data flow.
7. Choke packet technique is applicable to both virtual networks as well as datagram subnets. A choke packet is a packet sent by a node to the source to inform it of congestion.
8. When too many packets are present in a subnet (or part of a subnet), performance degrades. Packets sent are not equal to the packets received. This situation is called flow control.
9. IPv4 is a 32-bits IP address.
10. The address space of IPv4 is 2^{32} or 4,294,967,296.
11. A mask used to determine what subnet an IP address belongs to.
12. In a class C address, the first octet would always start with '10'. Thus, class C addresses range from 192.0.0.0 to 223.255.255.255.
13. Network Address Translation (NAT) is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts.
14. The supernets are created through the use of subnet masks.
15. The subset mask identifies which bits in the IP address are to be used to represent the network subnet portion of an IP address.
16. Gateways work on a network layer and provide mechanism to route data to its destination.
17. Mobile IP has two addresses for a mobile host (home address: permanent) it associates the host with its home network and Care-of address Changes as the mobile host moves from one network to another and it is associated with the foreign network.
18. Internet Protocol version 6 (IPv6) is the most recent version of the Internet Protocol (IP).
19. IPv6 is the next generation Internet Protocol (IP) standard intended to eventually replace IPv4.
20. Subnetting is the process of dividing (partitioning) a network into several smaller networks (subnets).

21. A router is a device that forwards packets between networks by processing the routing information included in the packet.
22. RIP (Routing Information Protocol) is the best example of a protocol using distance vector.
23. Subnetting, also called Classless Inter-Domain Routing (CIDR), is a way to aggregate multiple Internet addresses of the same class.
24. CIDR notation specifies the number of bits set to a 1 that make up the subnet mask.

ANSWERS

1. (T)	2. (F)	3. (T)	4. (F)	5. (T)	6. (T)
7. (T)	8. (F)	9. (T)	10. (T)	11. (T)	12. (F)
13. (T)	14. (F)	15. (T)	16. (F)	17. (T)	18. (T)
19. (T)	20. (T)	21. (T)	22. (T)	23. (F)	24. (T)

Q. IV Answer the following Questions:

(A) Short Answer Questions:

1. What are the services provided by the network layer?
2. List functions of the network layer.
3. What is flow and error control?
4. Define congestion. When it occurs.
5. List types of congestion control mechanisms.
6. What is an IP address?
7. List classes for classful IP addressing.
8. Define masking.
9. What is meant by subnetting?
10. Define supernetting.
11. What is meant by classless addressing/
12. What is NAT?
13. List network layer protocols.
14. What is fragmentation?
15. What is Mobile IP?
16. List three phases of Mobile IP.
17. What is IPv6?
18. List address for IPv6.
19. What is an extension header?
20. Define routing.

21. Give role of routing algorithm in routing.
22. List various routing algorithms.

(B) Long Answer Questions:

1. With the help of diagrams describe congestion control in the network layer.
2. Write a short note on: IPv4 addressing.
3. With the help of diagram and example describe format of an IP address.
4. Give address space for IPv4 and IPv6 addresses.
5. Describe classful addressing with diagrams.
6. Explain the term masking and subnet masking with example.
7. Explain supernetting with example.
8. Define NAT. How does it work? Explain with an example.
9. Describe forwarding IP packets based on destination address and based on label.
10. Describe IP protocol with datagram format.
11. Explain the term fragmentation with its related fields.
12. With the help of a diagram describe Mobile IP (MIP) architecture.
13. Define the terms HA and FA in MIP.
14. Explain phases of Mobile IP diagrammatically.
15. Describe IPv6 protocol with packer format.
16. Write a short note on: Extension header.
17. Differentiate between IPv4 and IPv6.
18. Define routing and routing algorithm.
19. With the help of example describe distance vector routing algorithm.
20. Describe link state routing algorithm with example.

UNIVERSITY QUESTIONS AND ANSWERS**April 2016**

1. Find out the class, Net ID and Host ID of IP address 126.47.50.23. [1 M]

Ans. Refer to Section 3.3.

2. Explain classful addressing in detail. [5 M]

Ans. Refer to Section 3.3.2.

3. List different task performed by the network layer. [2 M]

Ans. Refer to Section 3.0.

April 2017

1. Find out class, netid and hostid of IP address 126.25.21.1. [4 M]

Ans. Refer to Section 3.3.

October 2017

1. What is fragmentation?

[1 M]

Ans. Refer to Section 3.5.3.

2. State the class of the IP address 128.89.0.26.

[1 M]

Ans. Refer to Section 3.3.

3. Explain open and closed loop congestion control mechanisms.

[5 M]

Ans. Refer to Section 3.2, Points (1) and (2).

April 2018

1. Identify the class of the IP addresses 192.168.60.12 and 10.11.1.1.

[1 M]

Ans. Refer to Section 3.3.

2. Define subnetting.

[1 M]

Ans. Refer to Section 3.3.3.

3. What is routing? Explain the desirable characteristics.

[5 M]

Ans. Refer to Section 3.8.1.

October 2018

1. What is fragmentation?

[1 M]

Ans. Refer to Section 3.5.3.

2. Define routing.

[1 M]

Ans. Refer to Section 3.8.1.

3. What is congestion?

[5 M]

Ans. Refer to Section 3.2.

4. What are the services provided by the network layer?

[5 M]

Ans. Refer to Section 3.1.

5. List the congestion control policies used at the network layer.

[2 M]

Ans. Refer to Section 3.2.

April 2019

1. Convert dotted decimal IP address to binary address 255.255.0.0.

[1 M]

Ans. Refer to Section 3.3.

2. What is congestion?

[1 M]

Ans. Refer to Section 3.2.

3. Explain Host id and Net id of IP address classes.

[4 M]

Ans. Refer to Section 3.3.



Transport Layer

Objectives...

- To learn Transport Layer with its Services
- To study UDP and TCP Protocols

4.0 INTRODUCTION

- The transport layer is responsible for providing services to the application layer, it receives services from the network layer.
- Transport layer, (layer 4) in the TCP/IP model is responsible for process-to-process communication, flow control, congestion control and so on.
- The original TCP/IP protocol suite specifies two protocols for the transport layer namely, UDP and TCP.
- A new transport layer protocol SCTP is recently developed for signaling message transport over IP networks.

4.1 TRANSPORT LAYER SERVICES

- The transport layer provides communication services between the computers connected in the network.
- In this section, we discuss the services that can be provided by a transport layer like process-to-process communication, addressing, encapsulation and decapsulation, multiplexing and demultiplexing, flow control, congestion control and so on.

4.1.1 Process-to-Process Communication

- The first duty of a transport layer is to provide process-to-process communication. A process is an application program running on the host and uses the services of the transport layer.
- Before we discuss how process-to-process communication can be accomplished, we need to understand the difference between host-to-host communication and process-to-process communication.
- The data link layer is responsible for delivery of frames between two neighboring nodes over a link. This is called node-to-node communication.

- The network layer is responsible for delivery of datagram between two hosts. This is called host-to-host communication.
- Real communication takes place between two processes (application programs) in a network. This is called process-to process communication.
- The transport layer is responsible for process-to-process communication, the delivery of a packet, part of a message, from one process to another.
- A network layer protocol can deliver the message only to the destination computer. However, this is an incomplete delivery.
- The message still needs to be handed to the correct process. This is where a transport layer protocol takes over.
- A transport layer protocol is responsible for delivery of the message to the appropriate process.
- Fig. 4.1 shows the domains of a network layer and a transport layer.

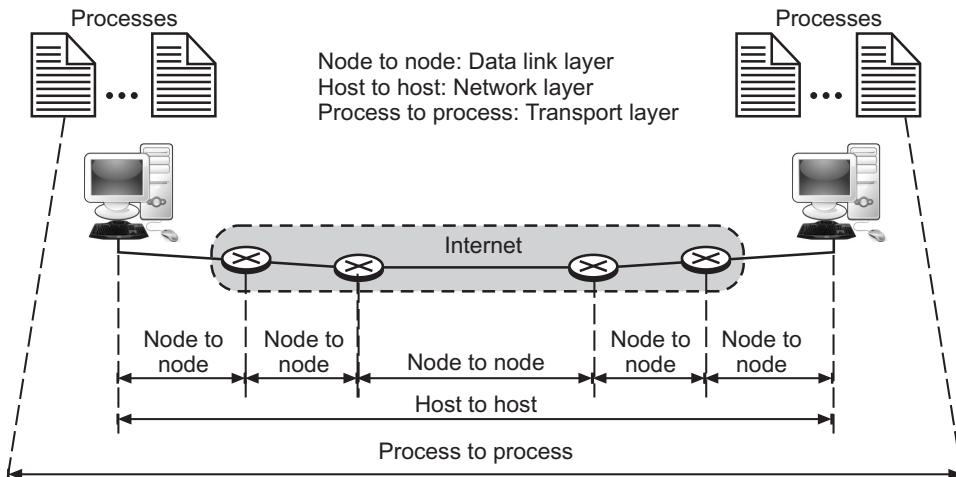


Fig. 4.1: Network Layer versus Transport Layer

4.1.2 Addressing: Port Numbers

- The most common method to achieve process to process communication is through the client/server paradigm.
- A process on the local host, called a client, needs services from a process on the remote host called a server.
- The client and server machines can run several applications programs simultaneously.
- Both processes (client and server) have the same name. For example, to get the day and time from a remote machine, we need a day time client process running on the local host and day time server process running on a remote machine.

- However, Operating Systems (OS) today support both multiuser and multiprogramming environments.
- A remote computer can run several server programs at the same time, just as several local computers can run one or more client programs at the same time.
- For communication, we must define the local host, local process, remote host, and remote process.
- The local host and the remote host are defined using IP addresses. To define the processes, we need second identifiers, called port numbers.
- In the TCP/IP protocol suite, the port numbers are integers between 0 and 65,535 (16 bits).
- Port numbers are 16 bit long that help identify which process is sending or receiving data on a host.
- The client program defines itself with a port number, called the ephemeral port number. The word 'ephemeral' means 'short lived' and is used because the life of a client is normally short.
- The server process must also define itself with a port number. This port number, however, cannot be chosen randomly.
- If the computer at the server site runs a server process and assigns a random number as the port number, the process at the client site that wants to access that server and use its services will not know the port number.
- TCP/IP has decided to use universal port numbers for servers; these are called well-known port numbers.
- Every client process knows the well-known port number of the corresponding server process.
- For example, while the Daytime client process uses an ephemeral (temporary) port number 52,000 to identify itself, the Daytime server process must use the well-known (permanent) port number 15 (See Fig. 4.2).

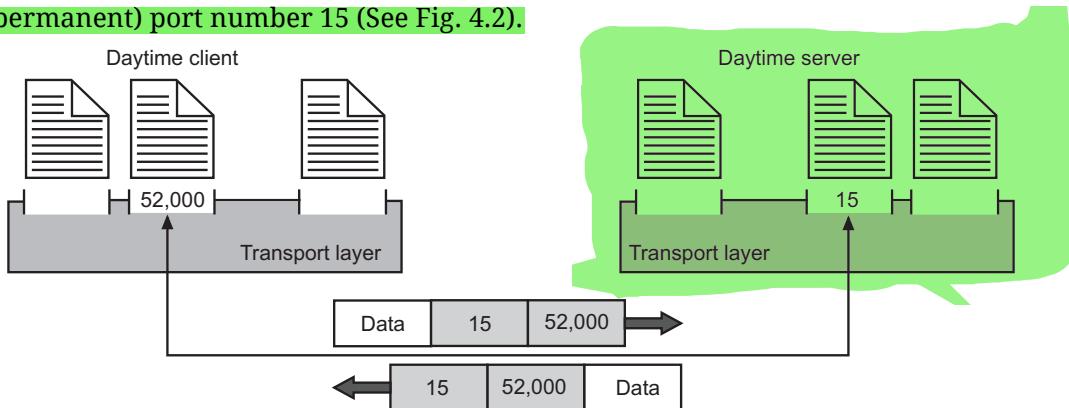


Fig. 4.2: Port Numbers

Addressing:

- To deliver the data, we need an address. At the data link layer, we need a physical (MAC) address. A frame in the data link layer needs a destination MAC address for delivery and source MAC address for reply.
- At the network layer, we need an IP address. A datagram in the network layer needs a destination IP address for delivery and a source IP address for the destination's reply.
- At the transport layer, we need a transport layer address called port address/number to choose among multiple processes running on the destination host.**
- The destination port number is needed for delivery; the source port number is needed for the reply.
- The IP addresses and port numbers play different roles in selecting the final destination of data. The role of destination IP address is to define the host among the different hosts.
- Once the host has been selected, the port number starts, the port number defines one of the processes on this particular host. This is shown in Fig. 4.3.

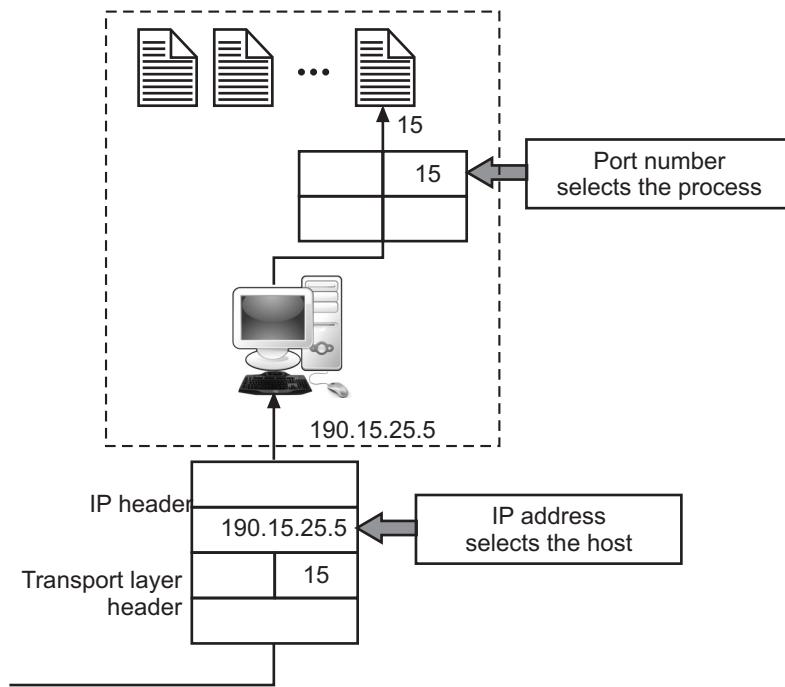


Fig. 4.3: The Role of Destination IP Address

IANA Ranges:

- The IANA (Internet Assigned Number Authority) has divided the port numbers into three ranges as shown in Fig. 4.4.

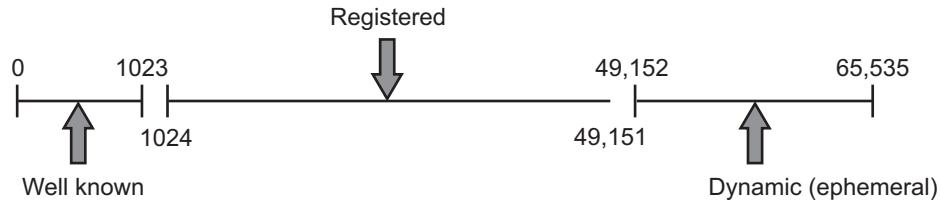


Fig. 4.4: IANA Ranges

- Fig. 4.4 shows following IANA Ranges:
 - Well Known Ports:** The ports from 0 to 1023 are assigned and controlled by IANA. These are well known ports.
 - Registered Ports:** The ports ranging from 1024 to 49151 are not assigned or controlled by IANA. They can be registered with IANA to avoid duplication.
 - Dynamic Ports (Ephemeral Ports):** The ports ranging from 49,152 to 65,535 are neither controlled nor registered. They can be used by any process. These are ephemeral ports.

Socket Addresses:

- Transport layer provides process-to-process communication which needs two identifiers, IP address and port number at each end to make a connection.
- The combination of an IP address and a port number is called a socket address.
- The client socket address shows the client process uniquely and the server socket address shows the server process uniquely.

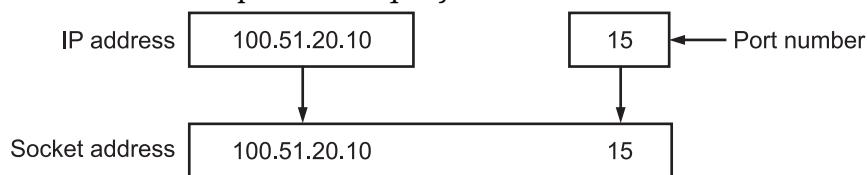


Fig. 4.5: Socket Address

4.1.3 Encapsulation and Decapsulation

- To send a message from one process to another, the transport layer encapsulates and decapsulates messages as shown in Fig. 4.6.
- Encapsulation happens at the sender site. When a process has a message to send, it passes the message to the transport layer along with a pair of socket addresses and some other pieces of information that depends on the transport layer protocol.
- The transport layer receives the data and adds the transport-layer header. The packets at the transport layers in the Internet are called user datagrams, segments, or packets.
- Decapsulation happens at the receiver site. When the message arrives at the destination transport layer, the header is dropped and the transport layer delivers the message to the process running at the application layer.

- The sender socket address is passed to the process in case it needs to respond to the message received.

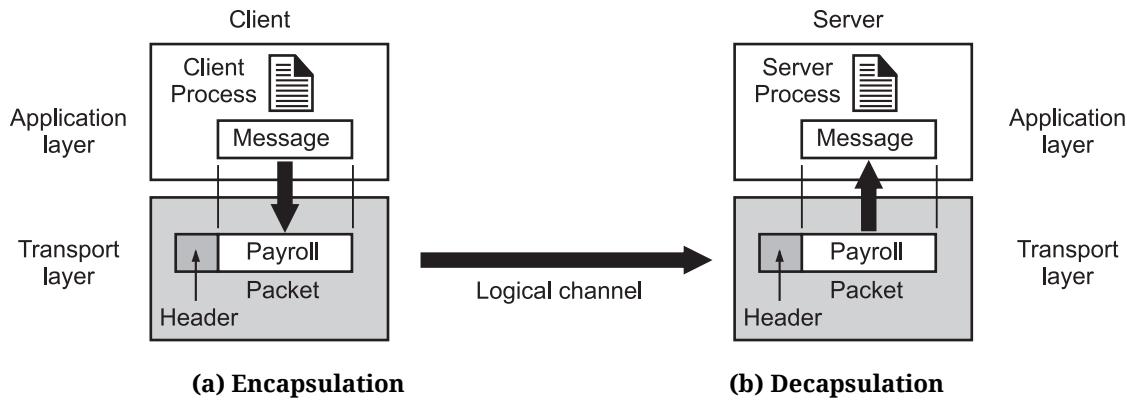


Fig. 4.6: Encapsulation and Decapsulation in Transport Layer

4.1.4 Multiplexing and Demultiplexing

(April 17)

- Multiplexing and demultiplexing are the two very important services that are performed by the transport layer.
- The transport layer at the source performs multiplexing while the transport layer at the destination performs demultiplexing as shown in Fig. 4.7.
- Whenever an entity accepts items from more than one source, it is referred to as multiplexing (many to one); whenever an entity delivers items to more than one source, it is referred to as demultiplexing (one to many).
- Fig. 4.7 shows communication between a client and two servers. Three client processes are running at the client site namely, P1, P2, and P3.
- The processes P1 and P3 need to send requests to the corresponding server process running in a server.
- The client process P2 needs to send a request to the corresponding server process running at another server.
- The transport layer at the client site accepts three messages from the three processes and creates three packets. It acts as a multiplexer.
- The packets 1 and 3 use the same logical channel to reach the transport layer of the first server.
- When they arrive at the server, the transport layer does the job of a multiplexer and distributes the messages to two different processes.
- The transport layer at the second server receives packet 2 and delivers it to the corresponding process.

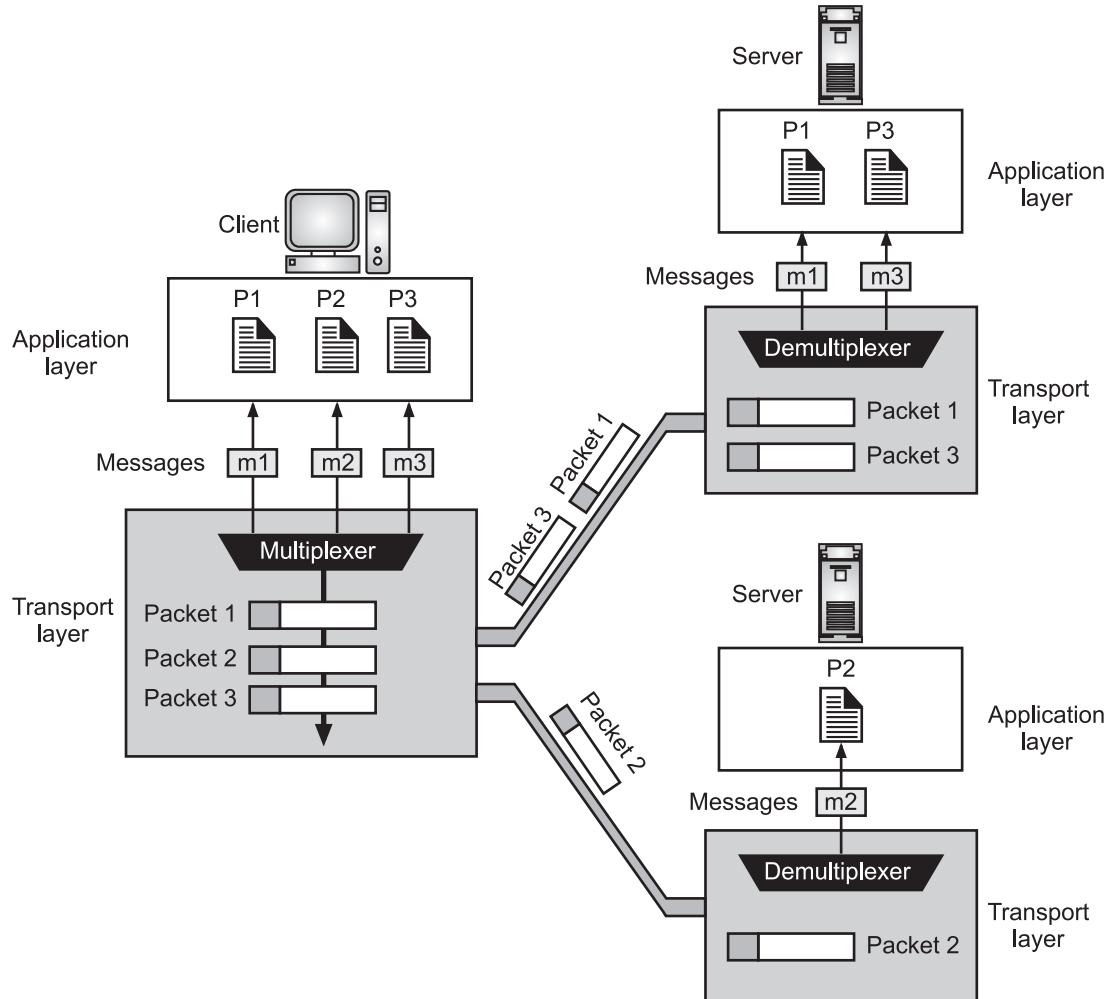


Fig. 4.7: Multiplexing and Demultiplexing

4.1.5 Flow Control

- The transport layer provides a flow control mechanism between the adjacent layers of the TCP/IP model.
- TCP also prevents data loss due to a fast sender and slow receiver by imposing some flow control techniques.
- In communication at the transport layer, we are dealing with four entities namely, sender process, sender transport layer, receiver transport layer, and receiver process.
- The sending process at the application layer is only a producer. It produces message chunks and pushes them to the transport layer.
- The sending transport layer has a double role, it is both a consumer and the producer. It consumes the messages pushed by the producer.

- It encapsulates the messages in packets and pushes them to the receiving transport layer.
- The receiving transport layer has also a double role, it is the consumer for the packets received from the sender. It is also a producer; it needs to decapsulate the messages and deliver them to the application layer.
- The last delivery, however, is normally a pulling delivery; the transport layer waits until the application-layer process asks for messages.
- Fig. 4.8 shows that we need at least two cases of flow control namely, from the sending transport layer to the sending application layer and from the receiving transport layer to the receiving transport layer.

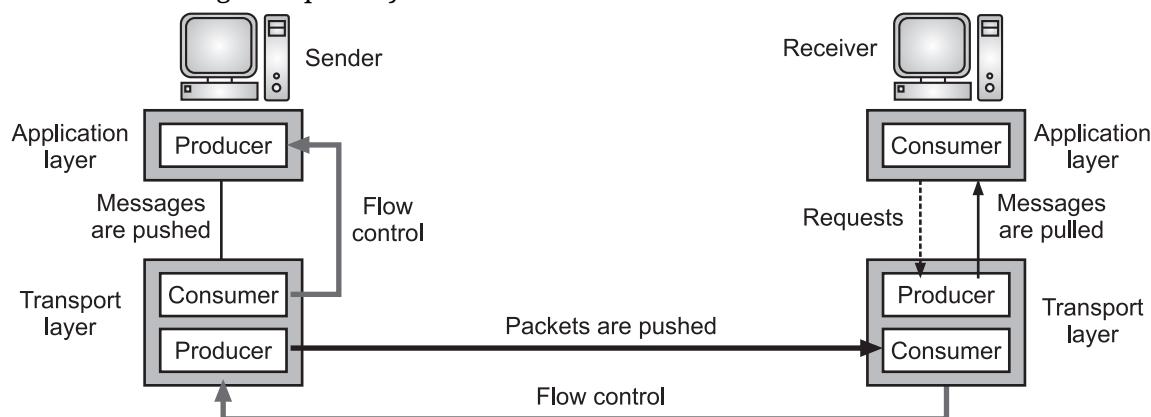


Fig. 4.8: Flow Control at the Transport Layer

4.1.5.1 Pushing or Pulling

- Delivery of items from a producer to a consumer can occur in one of the two ways namely, pushing or pulling.
 1. If the sender delivers items whenever they are produced without the prior request from the consumer the delivery is referred to as pushing.
 2. If the producer delivers the items after the consumer has requested them, the delivery is referred to as pulling.
- Fig. 4.9 shows above two types of delivery (pushing and pulling).

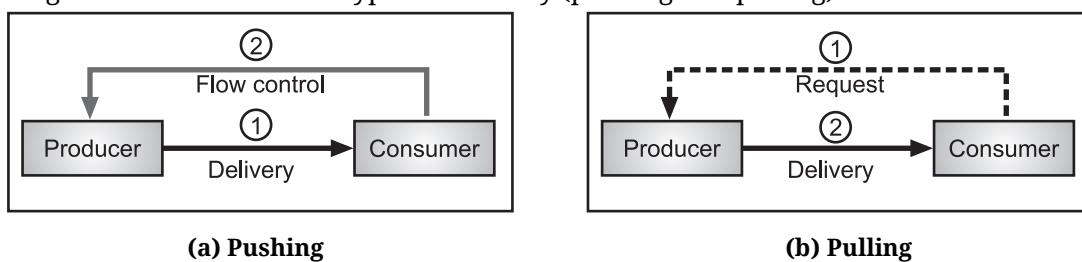


Fig. 4.9: Pushing and Pulling

- When the producer pushes the items, the consumer may be overwhelmed and there is a need for flow control, in the opposite direction, to prevent the discarding of the items.
- In other words, the consumer needs to warn the producer to stop the delivery and to inform it when it is ready again to receive the items.
- When the consumer pulls the items, it requests them when it is ready. In this case, there is no need for flow control.

4.1.5.2 Buffers

- Although flow control in the transport layer can be implemented in several ways, one of the solutions is normally to use two buffers. One at the sending transport layer and the other at the receiving transport layer.
- A buffer is a set of memory locations that can hold packets at the sender and receiver. The flow control communication can occur by sending signals from the consumer to producer.
- When the buffer of the sending transport layer is full, it informs the application layer to stop passing chunks of messages; when there are some vacancies, it informs the application layer that it can pass message chunks again.
- When the buffer of the receiving transport layer is full, it informs the sending transport layer to stop sending packets.
- When there are some vacancies, it informs the sending transport layer that it can send messages again.
- For example: The consumers communicate with the producers on two occasions such as, when the buffer is full and when there are vacancies. If the two parties use a buffer of only one slot, the communication can be easier. Assume that each transport layer uses one single memory location to hold a packet. When this single slot in the sending transport layer is empty, the sending transport layer sends a note to the application layer to send its next chunk; when this single slot in the receiving transport layer is empty, it sends an acknowledgment to the sending transport layer to send its next packet. As we will see later, this type of flow control, using a single-slot buffer at the sender and the receiver, is inefficient.

4.1.6 Error Control

- The error control service in the transport layer, observes that the data delivered to the receiver is error free and reliable.
- Reliability can be achieved to add error control service to the transport layer. Error control at the transport layer is responsible to:
 1. Detect and discard corrupted packets.

- 2. Keep track of lost and discarded packets and resend them.
- 3. Recognize duplicate packets and discard them.
- 4. Buffer out-of-order packets until the missing packets arrive.
- Error control involves only the sending and receiving transport layers. We are assuming that the message chunks exchanged between the application and transport layers are error free.
- Fig. 4.10 shows the error control between the sending and receiving transport layer.
- As with the case of flow control, the receiving transport layer manages error control, most of the time, by informing the sending transport layer about the problems.

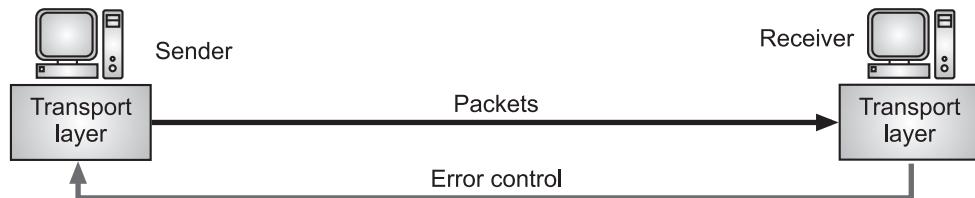


Fig. 4.10: Error Control at the Transport Layer

4.1.6.1 Sequence Numbers

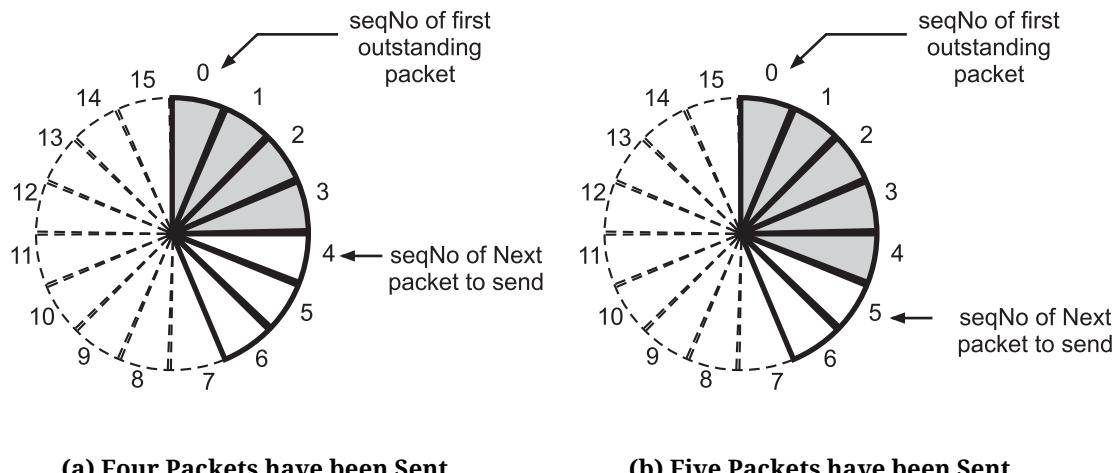
- Error control mechanism requires that the sending transport layer knows which packet is to be resent and the receiving transport layer knows which packet is a duplicate, or which packet has arrived out of order.
- This can be done if the packets are numbered. We can add a field to the transport layer packet to hold the sequence number of the packets.
- When a packet is corrupted or lost, the receiving transport layer can somehow inform the sending transport layer to resend that packet using the sequence number.
- The receiving transport layer can also detect duplicate packets if two received packets have the same sequence number. The out-of-order packets can be recognized by observing gaps in the sequence numbers.
- Packets are numbered sequentially. However, because we need to include the sequence number of each packet in the header, we need to set a limit.
- If the header of the packet allows m bits for the sequence number, the sequence numbers range from 0 to $2^m - 1$.
- For example, if m is 4, the only sequence numbers are 0 through 15, inclusive. However, we can wrap around the sequence. So the sequence numbers in this case are:
0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, ...
- In other words, the sequence numbers are modulo 2^m .

4.1.6.2 Acknowledgements

- In error control, we can use both positive and negative signals as error control. The receiver side can send an acknowledgement (ACK) for each or a collection of packets that have arrived safe and sound.
- The receiver can simply discard the corrupted packets. The sender can detect lost packets if it uses a timer.
- When a packet is sent, the sender starts a timer; when the timer expires, if an ACK does not arrive before the timer expires, the sender resends the packet.
- Duplicate packets can be silently discarded by the receiver. Out-of-order packets can be either discarded (to be treated as lost packets by the sender), or stored until the missing ones arrive.

4.1.6.3 Sliding Window

- Since the sequence numbers used modulo 2^m , a circle can represent the sequence number from 0 to $2^m - 1$ as shown in Fig. 4.11.
- The buffer is represented as a set of slices, called the sliding window, that occupy part of the circle at any time.
- At the sender site, when a packet is sent, the corresponding slice is marked. When all the slices are marked, it means that the buffer is full and no further messages can be accepted from the application layer.
- When an acknowledgment arrives, the corresponding slice is unmarked. If some consecutive slices from the beginning of the window are unmarked, the window slides over the range of the corresponding sequence number to allow more free slices at the end of the window.



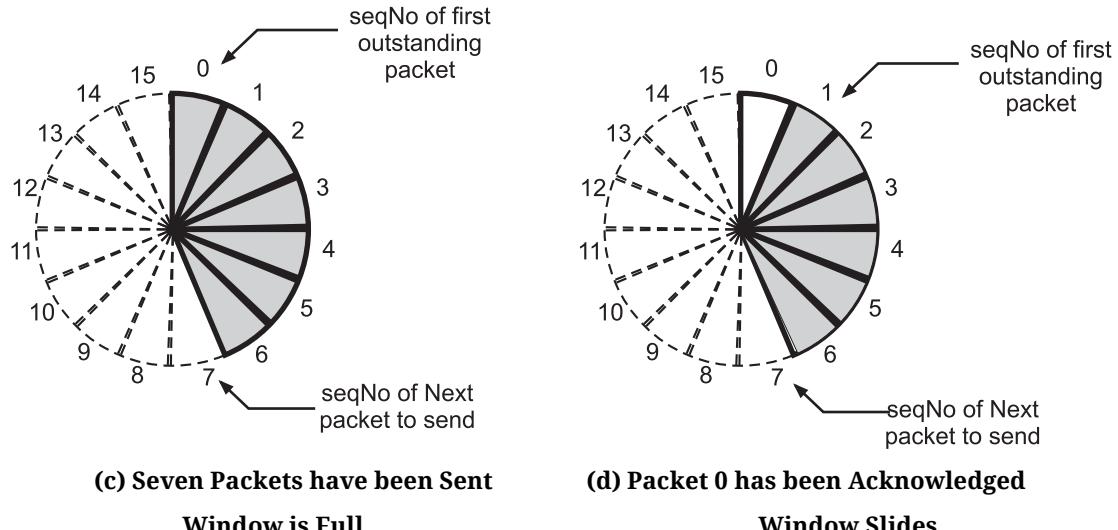


Fig. 4.11: Sliding Window in Circular Format

- Fig. 4.11 shows the sliding window at the sender. The sequence number are modulo 16 ($m = 4$) and the size of the window is 7.
- Note that the sliding window is just an abstraction: the actual situation uses computer variables to hold the sequence number of the next packet to be sent and the last packet sent.
- Number of protocols show the sliding window using linear representation. The idea is the same, but it normally takes less space on paper.
- Fig. 4.12 shows linear representation of the sliding window.

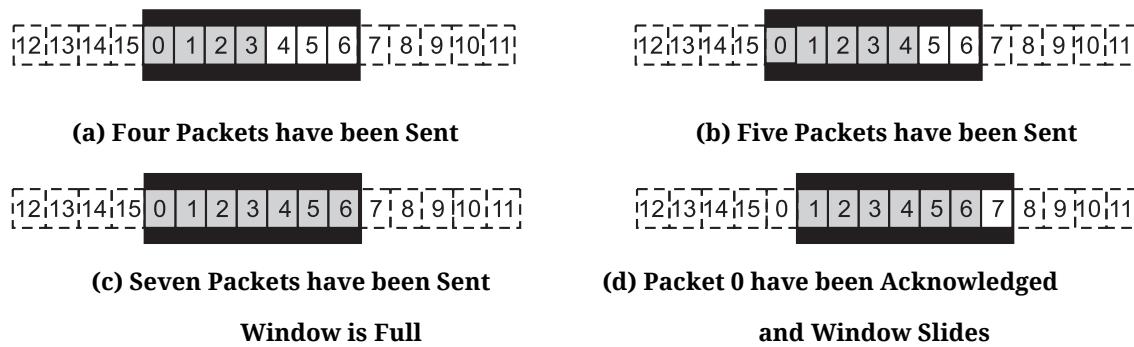


Fig. 4.12: Sliding Window in Linear Format

- Both representations (circular and linear) of the sliding window, tell us the same thing. If we take both sides of each part in Fig. 4.11 and bend them up, we can make the same part in Fig. 4.12.

4.1.7 Congestion Control

- Congestion is a situation in which too many sources over a network attempt to send data and the router buffers start overflowing due to which loss of packets occur.
- Congestion in a network may occur if the load on the network - the number of packets sent to the network - is greater than the capacity of the network - the number of packets a network can handle.
- Congestion control refers to the mechanisms and techniques to control the congestion and keep the load below the capacity.
- Congestion happens in any system that involves waiting. Congestion in a network or internetwork occurs because routers and switches have queues -buffers that hold the packets before and after processing.
- The packet is put in the appropriate output queue and waits its turn to be sent. These queues are finite, so it is possible for more packets to arrive at a router than the router can buffer.
- Congestion control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened.
- Congestion control uses open loop congestion control to prevent the congestion and closed loop congestion control to remove the congestion in a network once it occurs.

4.2

CONNECTIONLESS AND CONNECTION ORIENTED SERVICES

- A transport layer provides two types of services namely, connectionless and connection-oriented.
- 1. Connectionless Service:**
- In a connectionless service, the packets are sent from one machine to another without connection establishment or connection release.
 - The packets may arrive without order or they may be lost or delayed. Packets are not numbered. No acknowledgement is processed.
 - In a connectionless service, the source process (application program) needs to divide its message into chunks of data of the size acceptable by the transport layer and deliver them to the transport layer one by one.
 - The transport layer treats each chunk as a single unit without any relation between the chunks. When a chunk arrives from the application layer, the transport layer encapsulates it in a packet and sends it.
 - To show the independence of packets, assume that a client process has three chunks of messages to send a server process.

- The chunks are handed over to the connectionless transport protocol in order.
- However, since there is no dependency between the packets at the transport layer, the packets may arrive out of order at the destination and will be delivered out of order to the server process.
- In Fig. 4.13, we have shown the movement of packets using a timeline, but we have assumed that the delivery of the process to the transport layer and vice versa are instantaneous.
- The Fig. 4.13, shows that at the client site, the three chunks of messages are delivered to the client transport layer in order (1, 2, and 3).
- Because of the extra delay in transportation of the second packet, the delivery of messages at the server is not in order (1, 3, 2).
- If these three chunks (1, 2, and 3) of data belong to the same message, the server process may have received a strange message.

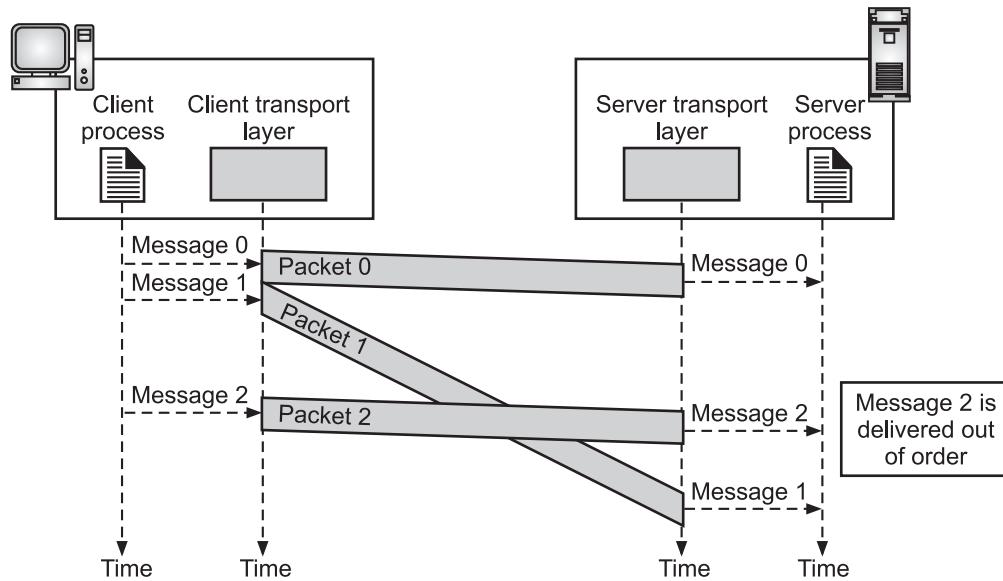


Fig. 4.13: Connectionless Service

- UDP is a transport layer's connectionless protocol.
- Connection Oriented Service:**
- In a connection oriented service, connection is established first and then data are transferred in between sender and receiver. After the end of data transfer, connection is released.
 - In a connection-oriented service, the client and the server first need to establish a connection between themselves.

- The data exchange can only happen after the connection establishment. After data exchange, the connection needs to be torn down as shown in Fig. 4.14.
- As we mentioned before, the connection-oriented service at the transport layer is different from the same service at the network layer.
- In the network layer, connection-oriented service means a coordination between the two end hosts and all the routers in between.
- At the transport layer, connection-oriented service involves only the two hosts; the service is end to end.
- This means that we should be able to make a connection-oriented protocol over either a connectionless or connection-oriented protocol.

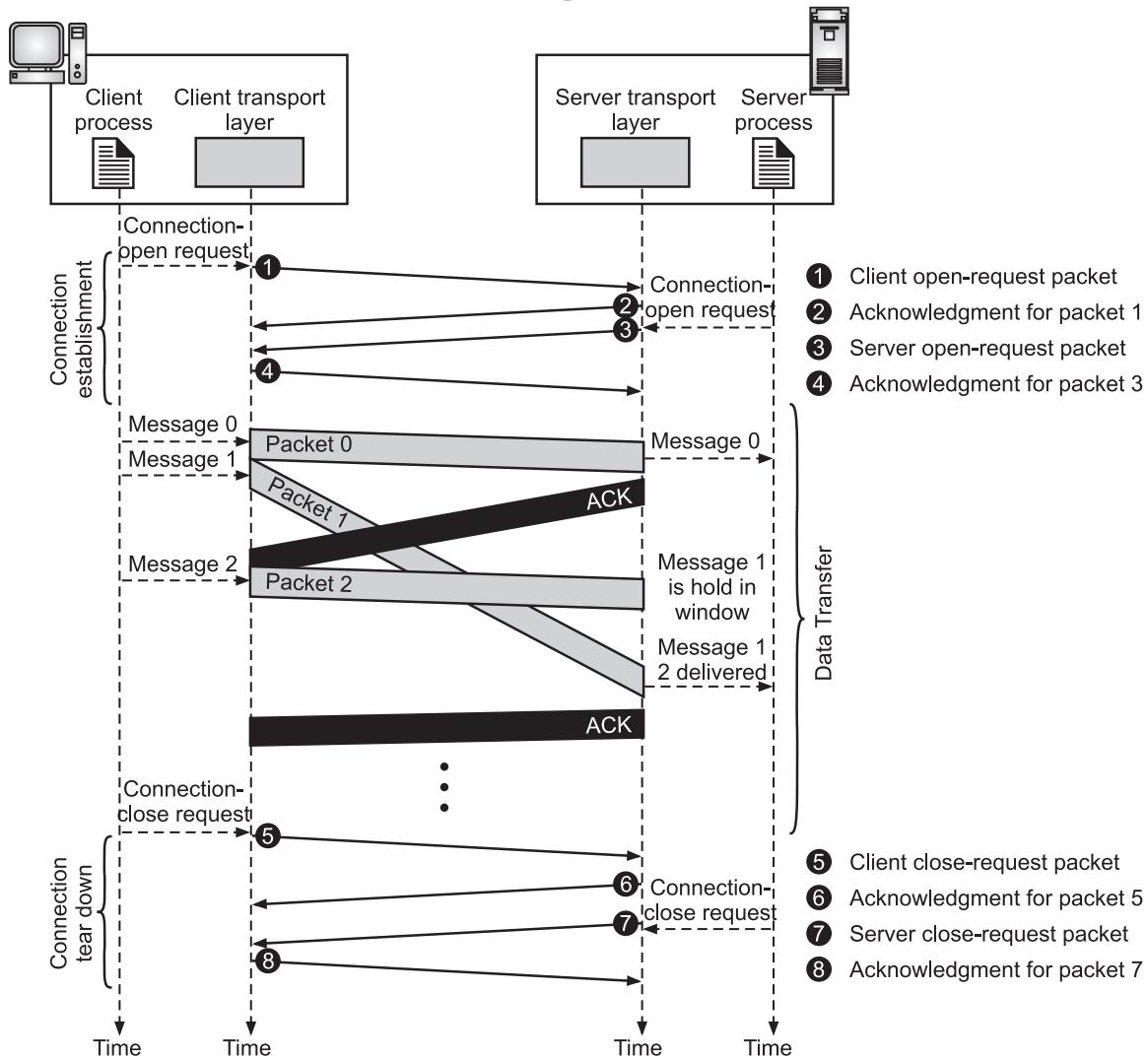


Fig. 4.14: Connection-oriented Service

- Fig. 4.14 shows the connection establishment, data transfer, and teardown phases in a connection-oriented service at the transport layer.
- Note that most protocols combine the third and fourth packets in the connection establishment phase into one packet.
- TCP and SCTP, these two transport layer protocols are connection oriented.

4.3 TRANSPORT LAYER PROTOCOLS

(Oct. 18)

- In the Internet protocol suite, the transport layer supports three protocols TCP, SCTP and UDP. Out of which TCP and SCTP are connection oriented and reliable and UDP is connectionless and unreliable.
- Fig. 4.15 shows the position of UDP, TCP and SCTP in the TCP/IP protocol suite.

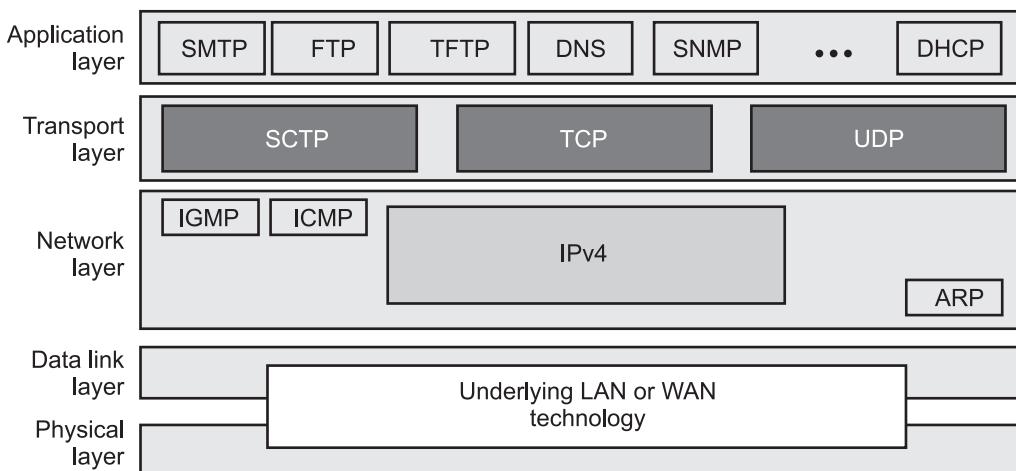


Fig. 4.15

4.3.1 User Datagram Protocol (UDP)

(April 16, 18)

- The User Datagram Protocol (UDP) is the simplest Transport Layer communication protocol in the TCP/IP protocol suite and serves as the intermediary between the application programs and the network operations.
- The UDP 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 powerless protocol. But it 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.

Features of UDP:

1. **Connectionless Service:** UDP provides connectionless service. In UDP each packet is independent from other packets sent by the same application.
2. **Lack of Congestion Control:** UDP does not provide congestion control and it does not create additional traffic in an error prone network.
3. **Lack of Error Control:** UDP does not provide error control. So UDP provides unreliable service.
4. **Transaction-oriented:** UDP is transaction-oriented, suitable for simple query-response protocols such as the Domain Name System (DNS).
5. **Datagram:** UDP provides datagrams, suitable for modeling other protocols such as IP tunneling or Remote Procedure Call (RPC) and the Network File System (NFS). An UDP datagram is used in Network File System (NFS), DNS, SNMP, TFTP etc.
6. **Simple:** UDP is a simple, datagram-oriented, transport-layer protocol. UDP is simple, suitable for bootstrapping or other purposes without a full protocol stack, such as the DHCP and Trivial File Transfer Protocol (TFTP).
7. **Stateless:** UDP is stateless, suitable for very large numbers of clients, such as in streaming media applications such as IPTV.
8. **Lack of Retransmission Delays:** The lack of retransmission delays makes UDP suitable for real-time applications such as Voice over IP, online games, and many protocols using Real Time Streaming Protocol.
9. **Support Multicast:** Because it supports multicast, it is suitable for broadcast information such as in many kinds of service discovery and shared information such as Precision Time Protocol (PTP) and Routing Information Protocol (RIP).
10. **Faster in Data Transfer:** UDP is a lightweight protocol for faster and simpler data transmissions.
11. **Queuing:** UDP is simple and suitable for query based communications. The Queues are associated with the ports in UDP.
12. **Low Overhead:** UDP is designed to provide application processes with the ability to transfer data with a minimal overhead.
13. **Port:** UDP uses that concept of port, which allows to distinguish the different applications running on a machine. Besides the datagram and its data, a UDP message contains a source port number and destination port number.
14. **No Acknowledgment/Not Reliable:** In UDP data are transmitted with no acknowledgment of whether it is received or not. UDP is thus not as reliable as TCP. UDP does not guarantee ordered delivery of data.

Uses of UDP:

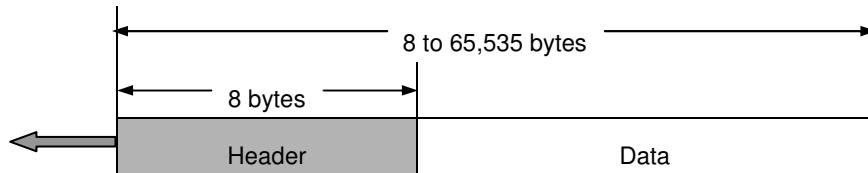
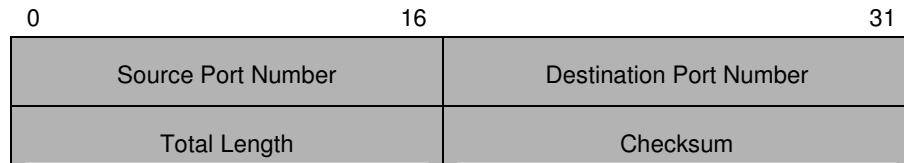
(Oct. 17)

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, TCP not.
5. UDP is used for management processes such as SNMP (Simple Network Management Protocol).

4.3.2 Datagram Format

(April 16, 19)

- UDP packets, called as user datagrams, have a fixed-size header of 8 bytes.
- Fig. 4.16 shows the format of a user datagram. Fig 4.17 shows header format of UDP.

**Fig. 4.16: UDP User Datagram****Fig. 4.17: Header Format of UDP**

- UDP header contains four main parameters:
 1. **Source Port Number:** This 16-bits field is used by the process running on the source host which wants to make communication. Port numbers can range from 0 to 65,535. If a client is sending a request, generally the port number is an ephemeral port number. If the server is sending a response port number is a well known port number.
 2. **Destination Port:** This 16-bits 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-bits 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-bits field is used to detect errors over the entire user datagram.

4.3.3 UDP Services

- The general UDP services are Process to Process Communication, Connectionless Services, Flow Control, Error Control, Congestion Control, Encapsulation and Decapsulation, Queuing, Multiplexing and Demultiplexing.

1. Process to Process Communication:

- UDP provides a process to process communication using sockets, a combination of IP addresses and port numbers.
- Several port numbers used by UDP are shown below:

Port No	Protocol	Description
7	Echo	Resends a received datagram back to the sender.
9	Discard	Discards a received datagram.
11	Users	Shows active users.
13	Daytime	Gives the date and time.
17	Quote	Gives a quote of the day.
19	Chargen	Gives a string of characters.
53	Nameserver	Shows Domain Name Service (DNS).
67	BOOTPs	Server port to download bootstrap information.
68	BOOTCPC	Client port to download bootstrap information.
69	TFTP	Trivial File Transfer Protocol (TFTP).
111	RPC	Remote Procedure Call.
123	NTP	Network Time Protocol.
161	SNMP	Simple Network Management Protocol.
162	SNMP	Simple Network Management Protocol.

2. Connectionless Services:

- UDP provides a connectionless service. This means that each user datagram sent by UDP is an independent datagram.

- In UDP there is no relationship between the different user datagrams even if they are coming from the same source process and going to the same destination program.
- The user datagrams are not numbered. There is no connection establishment and no connection termination as is the case for TCP.
- Each user datagram can travel on a different path. One of the ramifications of being connectionless is that the process that uses UDP cannot send a stream of data to UDP and expect UDP to chop them into different related user datagrams.
- Instead each request must be small enough to fit into one user datagram. Only those processes sending short messages, messages less than 65,507 bytes (65,535 minus 8 bytes for the UDP header and minus 20 bytes for the IP header), can use UDP.

3. Flow Control:

- UDP is a very simple protocol. There is no flow control, and hence no window mechanism. The receiver may overflow with incoming messages.
- The lack of flow control means that the process using UDP should provide for this service, if needed.

4. Error Control:

- There is no error control mechanism in UDP except for the checksum.
- Sender does not know if a message has been lost or duplicated. When the receiver detects an error through the checksum, the user datagram is silently discarded.
- The lack of error control means that the process using UDP should provide for this service if needed.

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.
- 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.

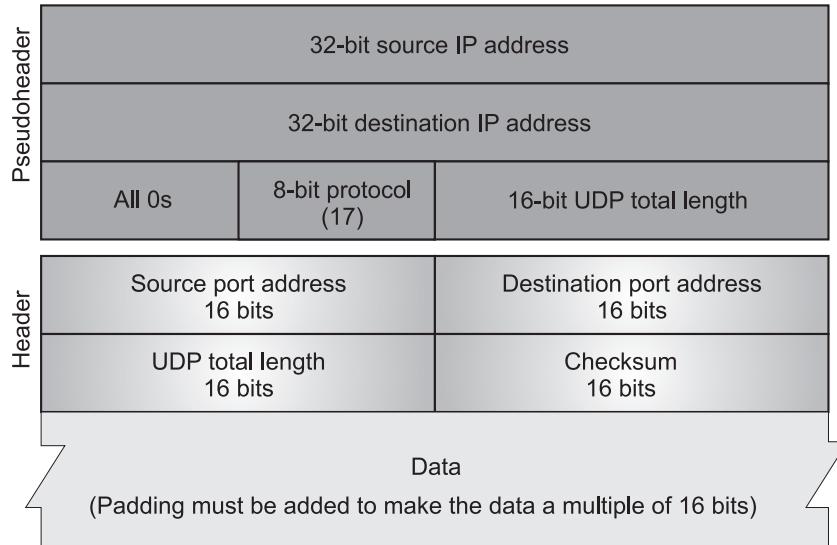


Fig. 4.18: Pseudo Header for Checksum Calculation

- 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. 4.19 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.

153.18.8.105		
171.2.14.10		
All 0s	17	15
1087		13
15		All 0s
T	E	S
I	N	G
All 0s		

10011001	00010010	→ 153.18
00001000	01101001	→ 8.105
10101011	00000010	→ 171.2
00001110	00001010	→ 14.10
00000000	00010001	→ 0 and 17
00000000	00001111	→ 15
00000100	00111111	→ 1087
00000000	00001101	→ 13
00000000	00001111	→ 15
00000000	00000000	→ 0 (checksum)
01010100	01000101	→ T and E
01010011	01010100	→ S and T
01001001	01001110	→ I and N
01000111	00000000	→ G and 0 (padding)
10010110	11101011	→ Sum
01101001	00010100	→ Checksum

Fig. 4.19: Checksum Calculation of a Simple UDP User Datagram

5. Multiplexing and Demultiplexing:

- In a host running a TCP/IP protocol suite, there is only one UDP but possibly several processes that may want to use the services of UDP. To handle this situation, UDP multiplexers and demultiplexers (See Fig. 4.20).

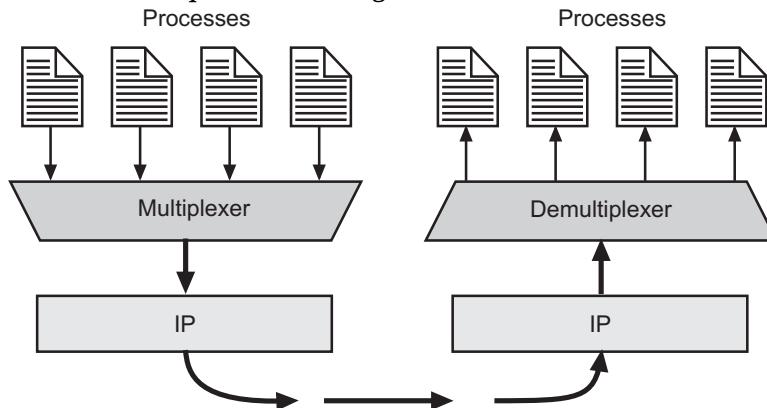


Fig. 4.20: Multiplexing and Demultiplexing

- UDP uses multiplexing to handle outgoing user datagrams from multiple processes on one host. UDP uses demultiplexing to handle incoming user datagrams that go to different processes on the same host.
- Multiplexing:** At the sender site, there may be several processes that need to send user datagrams. However, there is only one UDP. This is a many-to-one relationship and requires multiplexing. UDP accepts messages from different processes, differentiated by their assigned port numbers. After adding the header, UDP passes the user datagram to IP.
- Demultiplexing:** At the receiver site, there is only one UDP. However, we may have many processes that can receive user datagrams. This is a one-to-many relationship and requires demultiplexing. UDP receives user datagrams from IP. After error checking and dropping of the header, UDP delivers each message to the appropriate process based on the port numbers.

6. Encapsulation and Decapsulation:

- To send a message from one process to another, the UDP protocol encapsulates and decapsulates messages as shown in Fig. 4.21.

Encapsulation in UDP:

- When a process has a message to send through UDP, it passes the message to UDP along with a pair of socket addresses and the length of data.
- UDP receives the data and adds the UDP header. UDP then passes the user datagram to IP with the socket addresses.

- IP adds its own header, using the value 17 in the protocol field, indicating that the data has come from the UDP protocol.
- The IP datagram is then passed to the data link layer. The data link layer receives the IP datagram, adds its own header (and possibly a trailer), and passes it to the physical layer.
- The physical layer encodes the bits into electrical or optical signals and sends it to the remote machine.

Decapsulation in UDP:

- When the message arrives at the destination host, the physical layer decodes the signals into bits and passes it to the data link layer.
- The data link layer uses the header (and the trailer) to check the data. If there is no error, the header and trailer are dropped and the datagram is passed to IP.
- The IP software does its own checking. If there is no error, the header is dropped and the user datagram is passed to UDP with the sender and receiver IP addresses.
- UDP uses the checksum to check the entire user datagram. If there is no error, the header is dropped and the application data along with the sender socket address is passed to the process.
- The sender socket address is passed to the process in case it needs to respond to the message received.

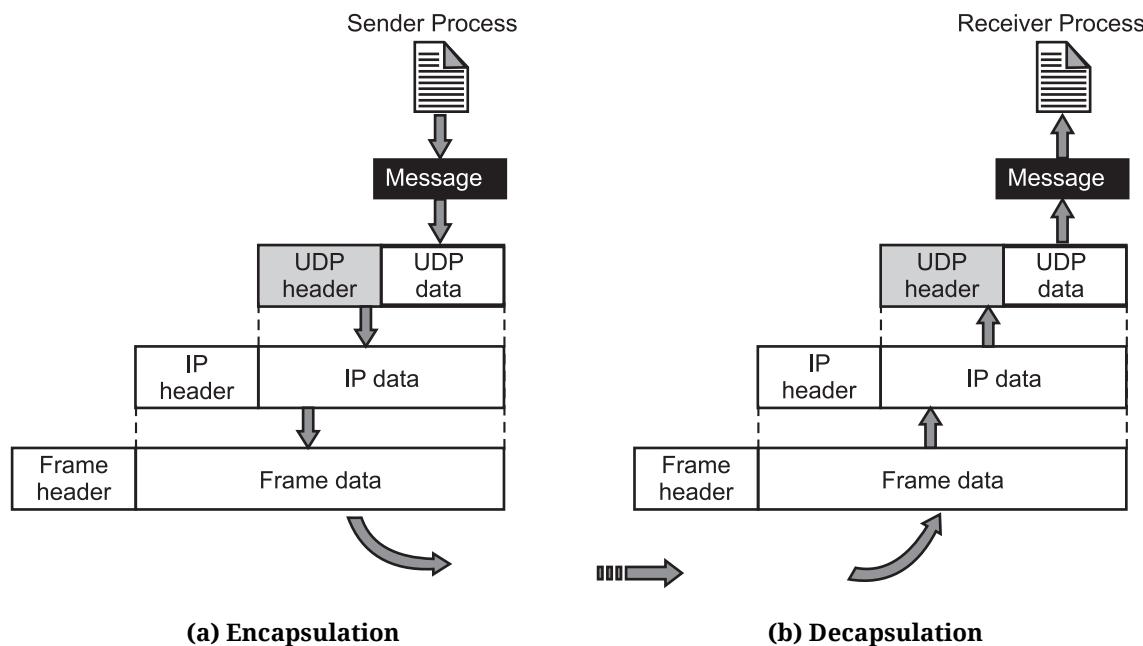


Fig. 4.21: Encapsulation and Decapsulation in UDP

7. Queuing:

- In UDP, queues are associated with ports as shown in Fig. 4.22.
- When a process starts, at the client site, it requests a port number from the Operating System (OS). Some implementations create both an incoming and an outgoing queue associated with each process while other implementations create only an incoming queue associated with each process.
- Even if a process wants to communicate with multiple processes, it obtains only one port number and eventually one outgoing and one incoming queue.
- The queues opened by the client are, in most cases, identified by ephemeral port numbers. The queues function 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 specified in the request.
- UDP removes the messages one by one, and after adding the UDP header, delivers them to IP. An outgoing queue can overflow.
- If this happens, the operating system can ask the client process to wait before sending any more messages.
- When a message arrives for a client, UDP checks to see if an incoming queue has been created for the port number specified in the destination port number field of the user datagram.
- If there is such a queue, UDP sends the received user datagram to the end of the queue. If there is no such queue, UDP discards the user datagram and asks the ICMP protocol to send a port unreachable message to the server.
- All of the incoming messages for one particular client program, whether coming from the same or a different server, are sent to the same queue. An incoming queue can overflow.
- If this happens, UDP drops the user datagram and asks for a port unreachable message to be sent to the server.
- At the server site, the mechanism of creating queues is different. In its simplest form, a server asks for incoming and outgoing queues using its well-known port when it starts running. The queues remain open as long as the server is running.
- When a message arrives for a server, UDP checks to see if an incoming queue has been created for the port number specified in the destination port number field of the user datagram.
- If there is such a queue, UDP sends the received user datagram to the end of the queue. If there is no such queue, UDP discards the user datagram and asks the ICMP protocol to send a port unreachable message to the client.

- All of the incoming messages for one particular server, whether coming from the same or a different client, are sent to the same queue.
- An incoming queue can overflow. If this happens, UDP drops the user datagram and asks for a port unreachable message to be sent to the client.
- When a server wants to respond to a client, it sends messages to the outgoing queue using the source port number specified in the request.
- UDP removes the messages one by one, and, after adding the UDP header, delivers them to IP.
- An outgoing queue can overflow. If this happens, the operating system asks the server to wait before sending any more messages.

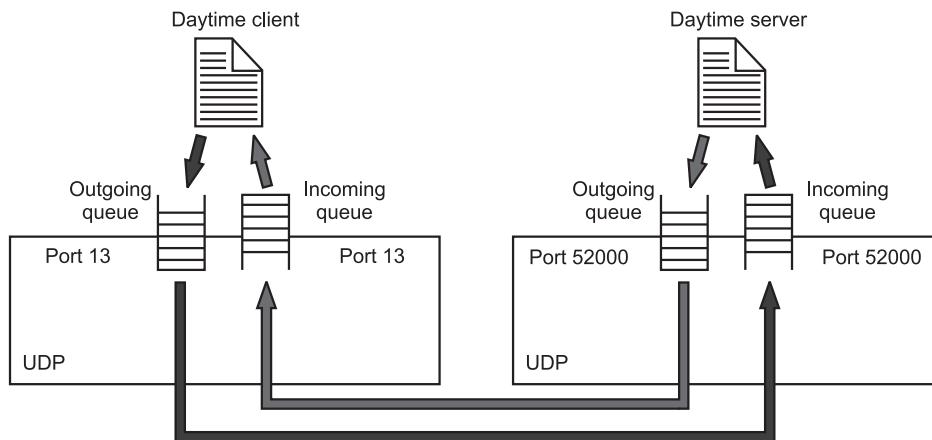


Fig. 4.22: Queuing in UDP

8. Congestion Control:

- UDP does not provide congestion control because it is a connectionless protocol. UDP assumes that the packets sent are small and sporadic, and cannot create congestion in the network.
- This UDP assumption may or may not be true today when UDP is used for real-time transfer of audio and video.

4.4

TRANSMISSION CONTROL PROTOCOL (TCP)

- The TCP is one of the most important protocols of the Internet Protocols suite. TCP is a reliable and connection oriented protocol.
- TCP is the most widely used protocol for data transmission in communication networks such as the Internet.
- TCP lies between the application layer and the network layer, and serves as the intermediary between the application programs and the network operations.

- TCP creates a virtual connection between two communicating entities/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 features to make TCP a reliable protocol.

4.4.1 TCP Services

(Oct. 18)

- The services offered by TCP to the process at the application layer are explained below:

1. Process-to-Process Communication:

- Like UDP, TCP provides process-to-process communication using port numbers.
- Port numbers are 16 bit long that help identify which process is sending or receiving data on a host.
- Table 4.1 shows some well-known port numbers used by TCP.

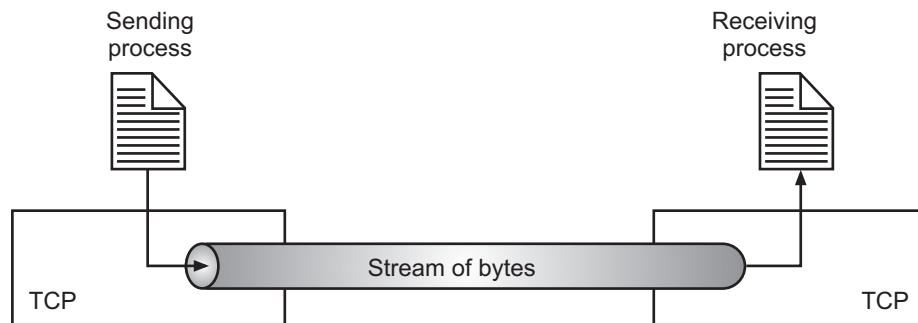
Table 4.1: Well-known ports used by TCP

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.
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.

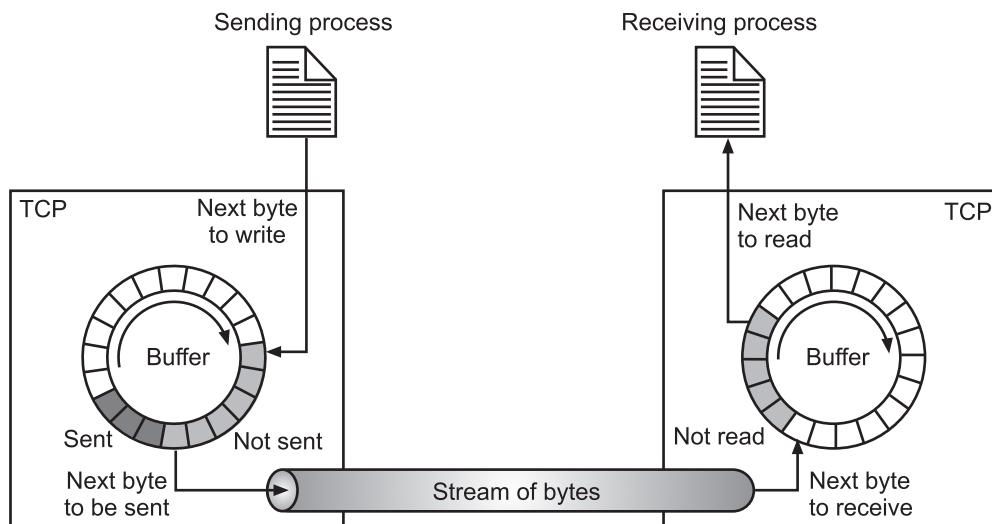
2. Stream Delivery Service:

(Oct. 17)

- 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. 4.23.
- The sending process produces the stream of bytes and the receiving process reads data from it.

**Fig. 4.23: 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 rate/speed.
- There are two buffers, sending buffer and receiving buffer, one for each.

**Fig. 4.24: Sending and Receiving Buffers**

- Fig. 4.24 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, and can be filled by the sending process.
- The cross-section area shows bytes are sent but not yet acknowledged. TCP keeps these bytes in the buffer until it receives an acknowledgement. The dotted area contains bytes to be sent by sending TCP.
- At receiver, the operation is simpler. The circular buffer is divided into two areas, white and shaded.
- The white area contains empty buffers to be filled by bytes received from the network layer.
- The shaded section contains received bytes that can be read by the receiving process. When the byte is read, that part of the buffer becomes empty.

4. Segments:

- Fig. 4.25 shows segments in TCP.
- The IP layer, as a service provider for TCP, needs to send data in packets, not as a stream of bytes. At the transport layer, TCP groups a number of bytes together into a packet called a segment.

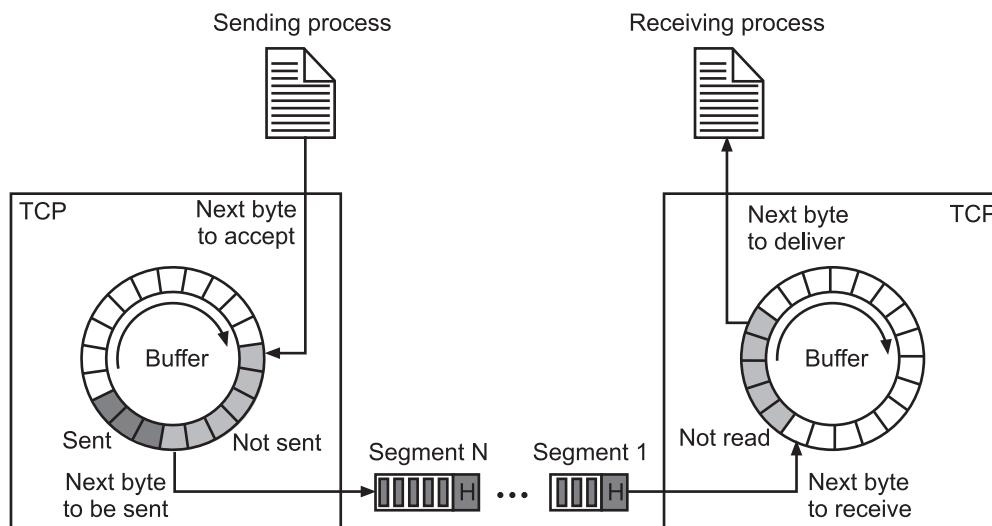


Fig. 4.25: TCP Segments

- 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.

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.

4.4.2 TCP Features

(April 17, 19)

- 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 is 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.

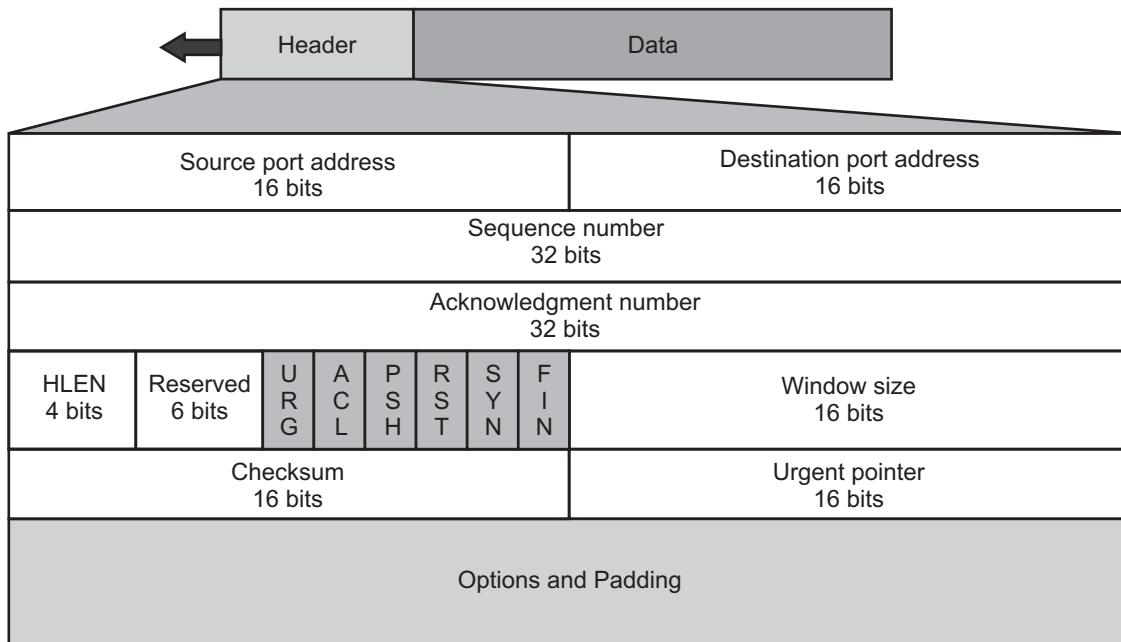
7. Congestion Control:

- 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.

4.4.3 TCP Segment Format

(April 18)

- A packet in TCP is called a segment. The format is shown in Fig. 4.26.

**Fig. 4.26: TCP Segment Format**

- The segment consists of a 20 to 60 bytes header, followed by data from the application layer.
- The header is of 20 bytes if no options are used and up to 60 bytes if it contains options.

- Fig. 4.26 shows following fields of TCP segment format:
 - Source Port Address:** This 16-bits field defines the port number of the application program in the host that is sending the segment.
 - Destination Port Address:** This 16-bits field defines the port number of the application program in the host who is receiving the segment.
 - Sequence Number:** This 32-bits field defines the number assigned to the first byte of data contained in the segment.
 - Acknowledgement Number:** This 32-bits field defines the byte number that the receiver of the segment is expecting to receive from another party.
 - Header Length:** This 4-bits field defines the length of the header. The length of the header can range between 20 to 60 bytes.
 - Reserved:** This 6-bits field is reserved for future use.
 - Control:** This field defines 6 different control bits or flags as shown in Fig. 4.27. One or more flags can be set at a time.

Note:

URG : Urgent pointer is valid	RST : Reset the connection
ACK : Acknowledgement is valid	SYN : Synchronize sequence number
PSH : Request for push	FIN : Terminate the connection

URG	ACK	PSH	RST	SYN	FIN
-----	-----	-----	-----	-----	-----

Fig. 4.27: 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 4.2.

Table 4.2: Description of flags 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.

- Windows Size: This 16-bits field defines the size of the window in bytes that another party 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-bits field contains the checksum used for error control.
10. **Urgent Pointer:** This 16-bits 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.

4.4.4 TCP Connection Establishment and Termination

- TCP is a connection oriented protocol and every connection oriented protocol needs to establish connection (a virtual path) in order to reserve resources at both the communicating ends i.e., source and destination.
- In TCP, connection-oriented transmission requires three phases namely, connection establishment, data transfer, and connection termination.

Connection Establishment:

- To establish a connection, TCP uses a three-way handshaking. Fig. 4.28 shows an example of connection establishment using three-way handshaking.
- In this example we take an application program, known as the client, wants to make a connection with another application program, known as the server, using TCP as the transport layer protocol.
- The process starts with the server. The server program tells its TCP that it is ready to accept a connection. This request is called a passive open.
- Although the server TCP is ready to accept a connection from any machine in the world, it cannot make the connection itself.
- The client program issues or initiates a request for an active open. A client that wishes to connect to an open server tells its TCP to connect to a particular server.
- TCP can now start the three-way handshaking process as shown in Fig. 4.28. To establish a connection, the three-way (or 3-step) handshake occurs:
 1. **SYN Segment:** In this segment only the SYN flag is set. SYN segment is for synchronization of sequence numbers. The client in the example chooses a random number as the first sequence number and sends this number to the server. This sequence number is called the Initial Sequence Number (ISN). The SYN segment is a control segment and carries no data. However, it consumes one sequence number. When the data transfer starts, the ISN is incremented by 1. We

can say that the SYN segment carries no real data, but we can think of it as containing one imaginary byte.

2. **SYN+ACK Segment:** It sets two flag bits set namely, SYN and ACK. A SYN + ACK segment cannot carry data, but does consume one sequence number. SYN-ACK segment has a dual purpose. First, it is a SYN segment for communication in the other direction. The server uses this segment to initialize a sequence number for numbering the bytes sent from the server to the client. The server also acknowledges the receipt of the SYN segment from the client by setting the ACK flag and displaying the next sequence number it expects to receive from the client. Because it contains an acknowledgment, it also needs to define the receive window size.
3. **ACK Segment:** ACK segment acknowledges the receipt of the second segment with the ACK flag and acknowledgment number field. An ACK segment, if carrying no data, consumes no sequence number.

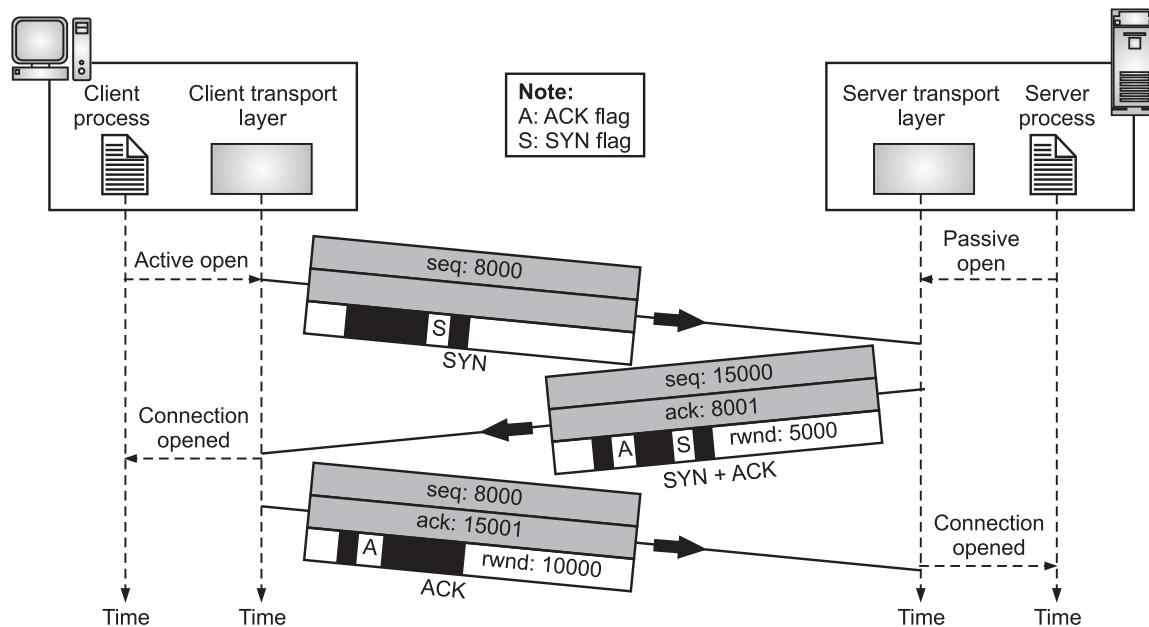


Fig. 4.28: Connection Establishment of TCP using Three-way Handshaking

Data Transfer in TCP:

- After connection of TCP is established, bidirectional data transfer can take place. The client and server can send data and acknowledgments in both directions.
- Fig. 4.29 shows an example of TCP in which, after a connection is established, the client sends 2,000 bytes of data in two segments. The server then sends 2,000 bytes in one segment.

- The client sends one more segment. The first three segments carry both data and acknowledgment, but the last segment carries only an acknowledgment because there is no more data to be sent.
- The data segments sent by the client have the PSH (push) flag set so that the server TCP tries to deliver data to the server process as soon as they are received.
- The segment from the server, on the other hand, does not set the push flag. Most TCP implementations have the option to set or not set this flag.

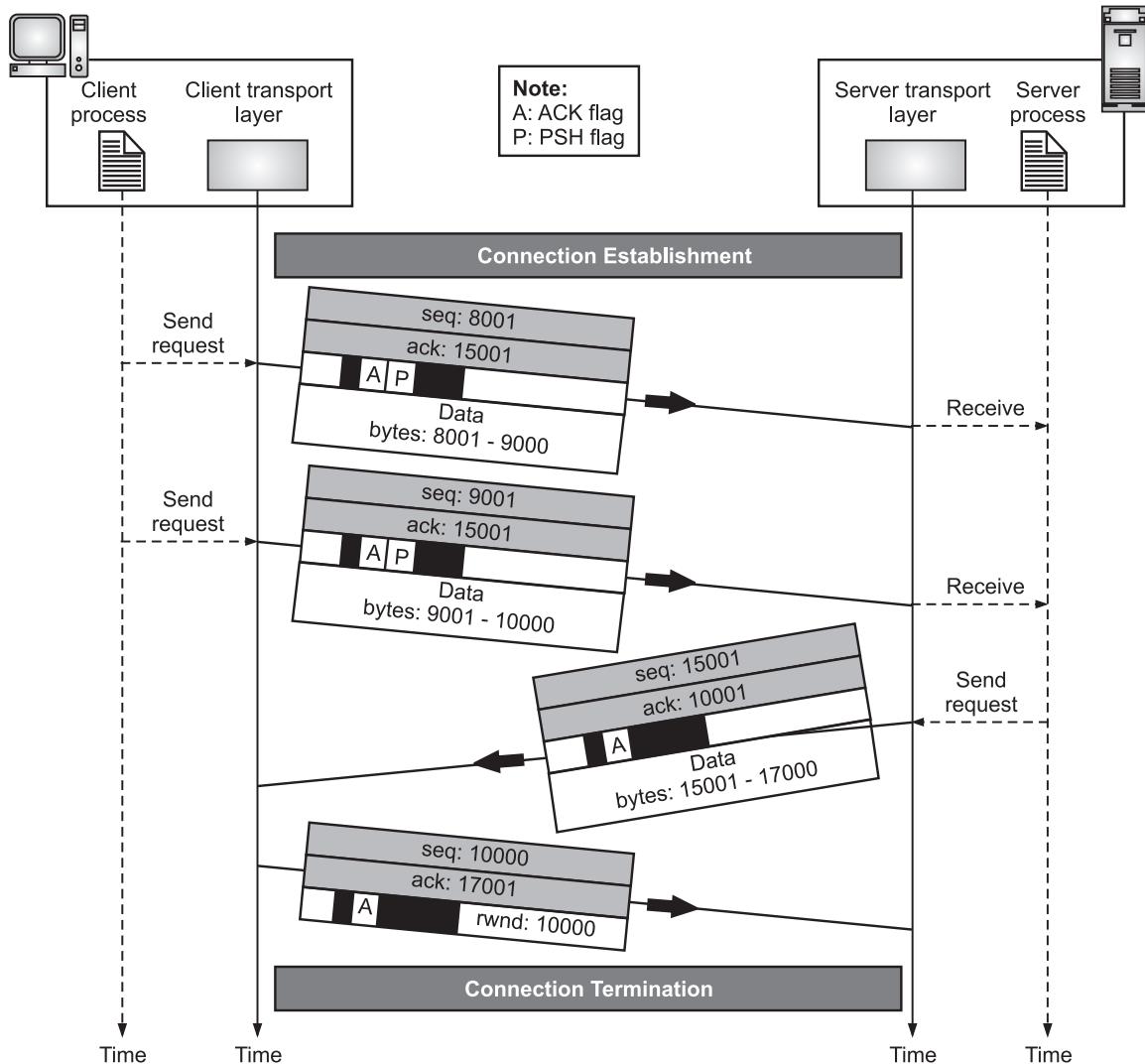


Fig. 4.29: Data Transfer in TCP

Connection Termination:

- Any of the two parties involved in exchanging/transferring data i.e., client or server can close the connection, although it is usually initiated by the client.

- Most implementations today allow two options for connection termination for TCP namely, three-way handshaking and four-way handshaking with a half-close option.

Three-Way Handshaking:

- Fig. 4.30 shows three-way handshaking for connection termination for TCP.
 - FIN Segment:** In a common situation, the client TCP, after receiving a close command from the client process, sends the first segment, a FIN segment in which the FIN flag is set. The FIN segment consumes one sequence number if it does not carry data.
 - FIN+ACK Segment:** The server TCP, after receiving the FIN segment, informs its process of the situation and sends the second segment, a FIN+ACK segment, to confirm the receipt of the FIN segment from the client and at the same time to announce the closing of the connection in the other direction. This segment can also contain the last chunk of data from the server. If it does not carry data, it consumes only one sequence number. The FIN + ACK segment consumes one sequence number if it does not carry data.
 - ACK Segment:** The client TCP sends the last segment, an ACK segment, to confirm the receipt of the FIN segment from the TCP server. This segment contains the acknowledgment number, which is one plus the sequence number received in the FIN segment from the server. This segment cannot carry data and consumes no sequence numbers.

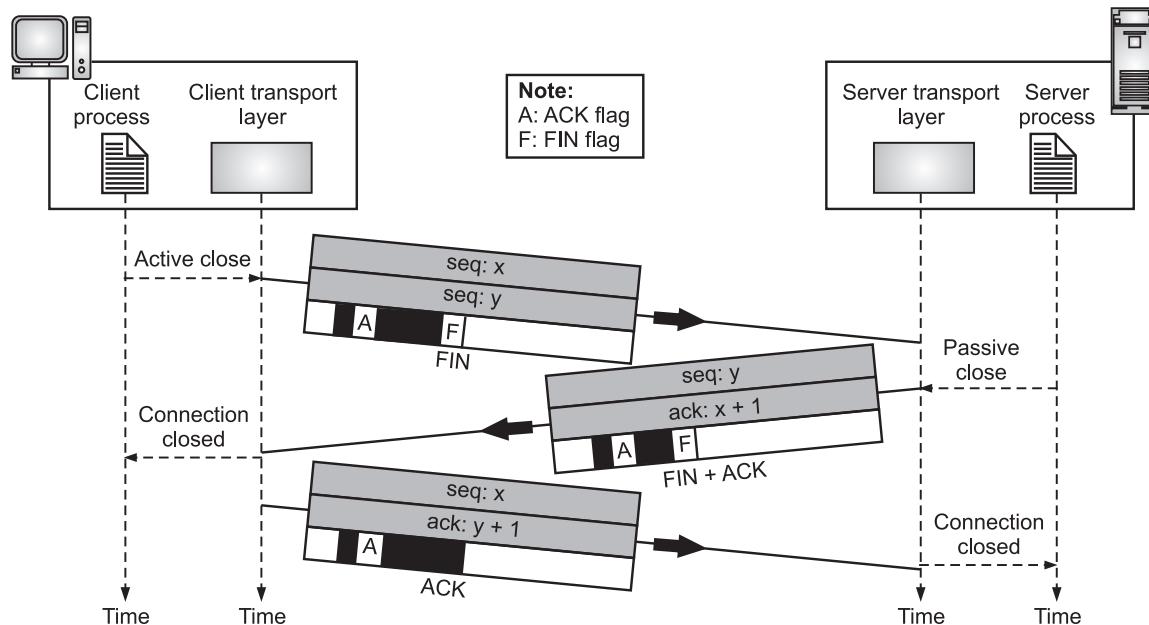


Fig. 4.30

4.4.5 State Transition Diagram

- To keep track of all the different events happening during TCP connection establishment, connection termination, and data transfer, TCP is specified as the finite state machine shown in Fig. 4.31.
- The Fig. 4.31 shows the two FSMs (Finite State Machines (a mathematical model of computation)) used by the TCP client and server combined in one diagram.
- In the Fig. 4.31, the ovals represent the states. The transition from one state to another is shown using directed lines. Each line has two strings separated by a slash. The first string is the input, which TCP receives. The second is the output, what TCP sends.
- The dotted black lines in the Fig. 4.31 represents the transition that a server normally goes through; the solid black lines show the transitions that a client normally goes through. However, in some situations, a server transitions through a solid line or a client transitions through a dotted line.
- The dark black lines show special situations. Note that the oval marked as ESTABLISHED is in fact two sets of states, a set for the client and another for the server, that are used for flow and error control.
- Following table list of states for TCP:

Sr. No.	State	Description
1.	CLOSED	No connection exists.
2.	LISTEN	Passive open received; waiting for SYN.
3.	SYN-SENT	SYN sent; waiting for ACK.
4.	SYN-RCVD	SYN+ACK sent; waiting for ACK.
5.	ESTABLISHED	Connection established; data transfer in progress.
6.	FIN-WAIT-1	First FIN sent; waiting for ACK.
7.	FIN-WAIT-2	ACK to first FIN received; waiting for second FIN.
8.	CLOSE-WAIT	First FIN received, ACK sent; waiting for application to close.
9.	TIME-WAIT	Second FIN received, ACK sent; waiting for 2MSL timeout.
10.	LAST-ACK	Second FIN sent; waiting for ACK.
11.	CLOSING	Both sides decided to close simultaneously.

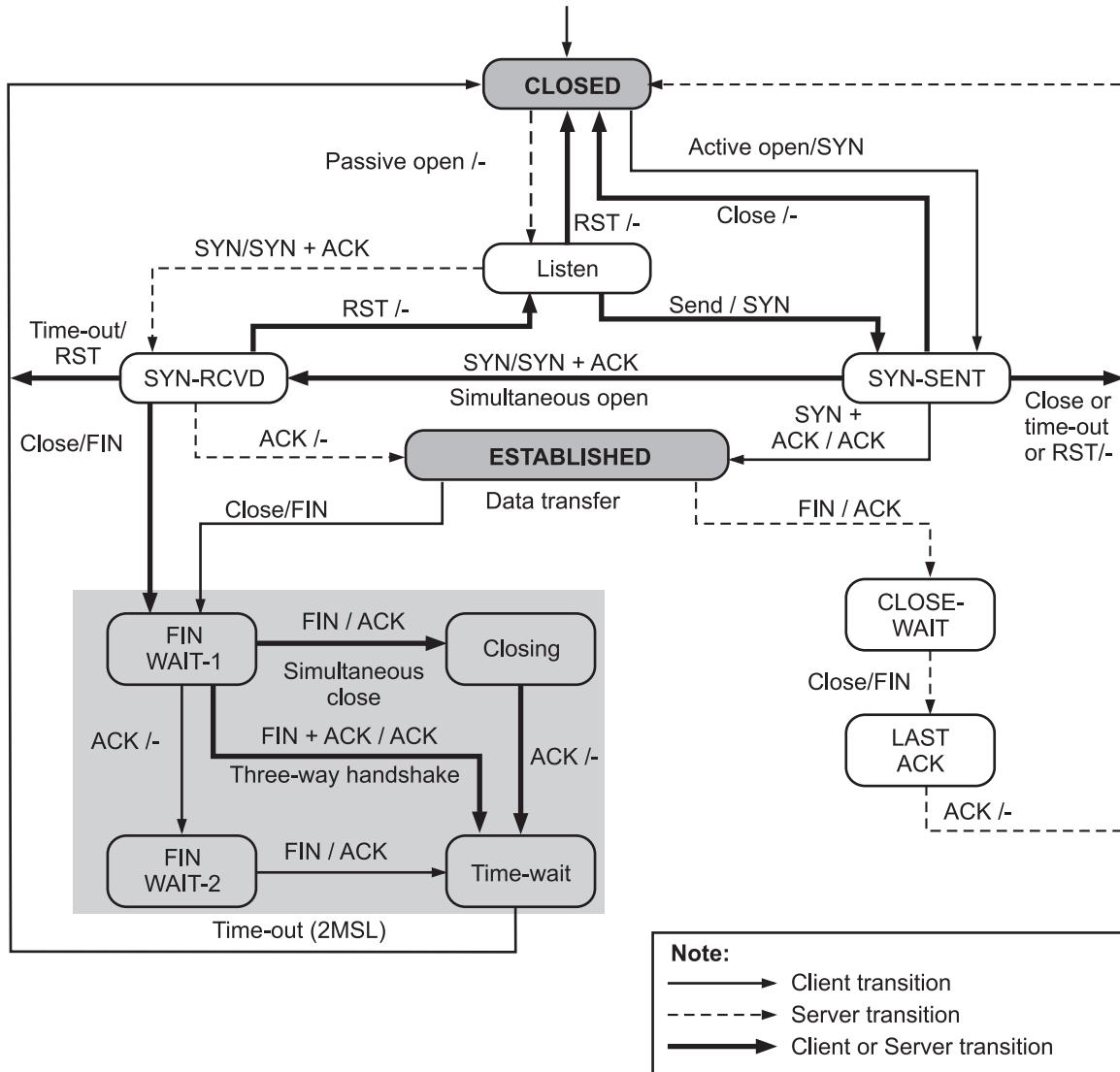
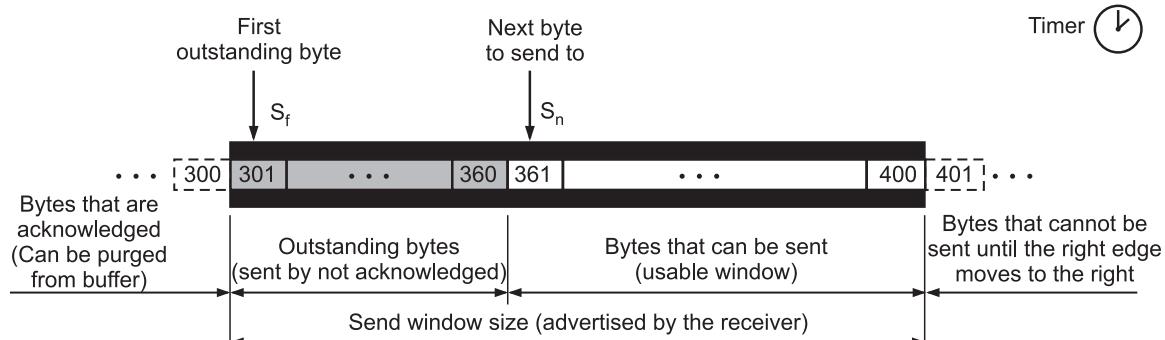


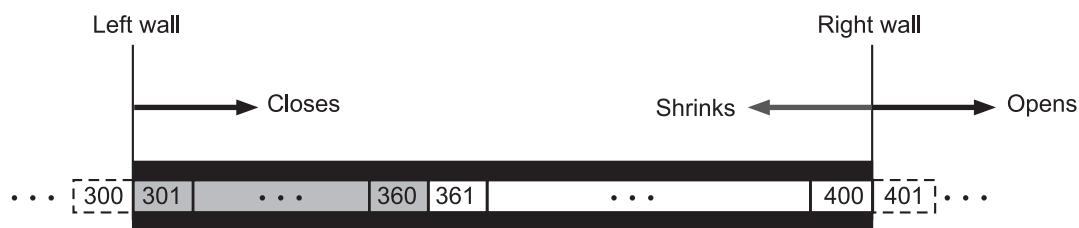
Fig. 4.31: State Transition Diagram of TCP

4.4.6 Windows in TCP

- TCP uses two windows (send window and receive window) for each direction of data transfer, which means four windows for a bi-directional communication.
1. **Send Window:**
- The window we have used is of size 100 bytes (normally thousands of bytes), but later we see that the send window size is dictated by the receiver (flow control) and the congestion in the underlying network (congestion control).



(a) Send Window



(b) Opening, Closing and Shrinking Send Window

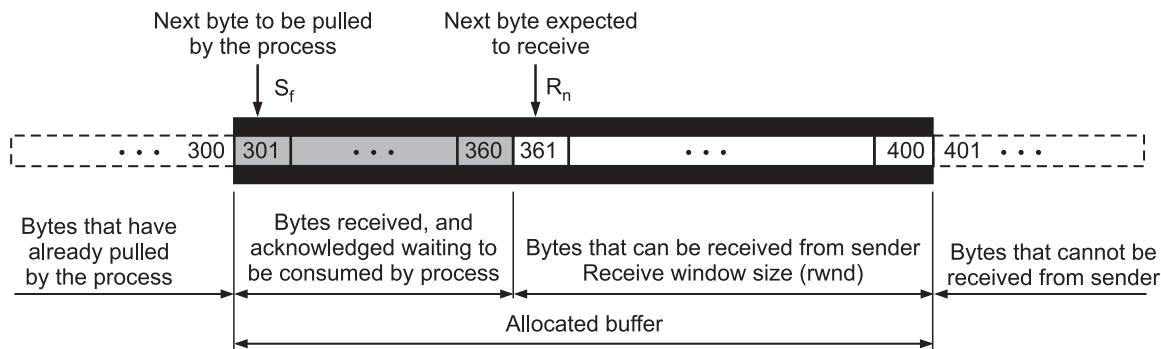
Fig. 4.32: Send Window in TCP

- The send window in TCP is similar to one used with the Selective Repeat (SR) protocol but with some following differences:
 - The nature of entities related to the window. The window in SR numbers packets, but the window in the TCP numbers bytes. Although actual transmission in TCP occurs segment by segment, the variables that control the window are expressed in bytes.
 - The second difference is that, in some implementations, TCP can store data received from the process and send them later, but we assume that the sending TCP is capable of sending segments of data as soon as it receives them from its process.
 - Another difference is the number of timers. The theoretical SR protocol may use several timers for each packet sent, but the TCP protocol uses only one timer.

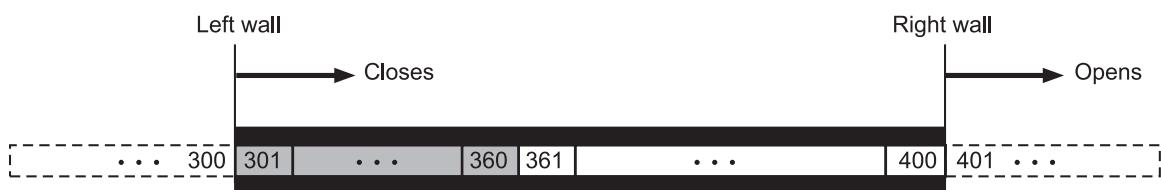
2. Receive Window:

- The window we have used is of size 100 bytes (normally thousands of bytes). The figure also shows how the receive window opens and closes; in practice, the window should never shrink.

- There are two differences between the receive window in TCP and the one we used for SR. These differences are given below:
 - The first difference is that TCP allows the receiving process to pull data at its own pace. This means that part of the allocated buffer at the receiver may be occupied by bytes that have been received and acknowledged, but are waiting to be pulled by the receiving process. The receive window size is then always smaller or equal to the buffer size, as shown in the Fig. 4.33. The receiver window size determines the number of bytes that the receive window can accept from the sender before being overwhelmed (flow control). In other words, the receive window size, normally called rwnd. It can be determined as $rwnd = \text{buffer size} - \text{number of waiting bytes to be pulled}$.
 - The way acknowledgments are used in the TCP protocol. Remember that an acknowledgement in SR is selective, defining the uncorrupted packets that have been received. The major acknowledgment mechanism in TCP is a cumulative acknowledgment announcing the next expected byte to receive. The new versions of TCP, however, uses both cumulative and selective acknowledgements.



(a) Receive Window and Allocated Buffer



(b) Opening and Closing of Receive Window

Fig. 4.33: Receive Window in TCP

Difference between TCP and UDP: (Oct. 18)

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 any user data can be sent. TCP handles reliability and congestion control.	UDP is lightweight. There is no ordering of messages, no tracking connections, 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.

PRACTICE QUESTIONS

Q.I Multiple Choice Questions:

1. The functions of transport layer of TCP/IP model include,

(a) Flow control	(b) Congestion control
(c) Addressing	(d) All of these
2. Which is an application program running on the host and uses the services of the transport layer?

(a) Datagram	(b) Packet
(c) Process	(d) None of these
3. Which is the most common method to achieve process to process communication?

(a) Web paradigm	(b) Client/server paradigm
(c) Programming paradigm	(d) None of these
4. Which numbers are 16 bit long that help identify which process is sending or receiving data on a host?

(a) Port	(b) Packet
(c) Message	(d) None of these
5. The transport layer address is called _____.

(a) Port address	(b) Port number
(c) Both (a) and (b)	(d) None of these
6. The IANA (Internet Assigned Number Authority) has divided the port numbers into three ranges,

(a) Well known ports	(b) Registered ports
(c) Dynamic ports	(d) All of these
7. Which is an address combination of IP address and a port number?

(a) Port address	(b) Logical number
(c) Socket address	(d) None of these
8. Which is a set of memory locations that can hold packets at the sender and receiver?

(a) Buffer	(b) Packet
(c) Message	(d) All of these
9. Which is a service in the transport layer, observes that the data delivered to the receiver is error free and reliable?

(a) Flow	(b) Congestion
(c) Error	(d) None of these

10. In which service, the packets are sent from one machine to another without connection establishment.
- (a) Connection-oriented (b) Connectionless
(c) Flow-oriented (d) All of these
11. Transport layer protocols include,
- (a) TCP (b) SCTP
(c) UDP (d) All of these
12. Which is connectionless, unreliable transport layer protocol?
- (a) TCP (b) SCTP
(c) UDP (d) All of these
13. UDP packets have a fixed-size header of _____ bytes.
- (a) 16 (b) 8
(c) 32 (d) 64
14. Which is the most widely used protocol for data transmission in communication networks as the Internet?
- (a) IP (b) UDP
(c) TCP (d) SCTP
15. Services of TCP include,
- (a) Flow control (b) Error control
(c) Congestion control (d) All of these
16. A packet in TCP is called _____.
- (a) Segment (b) Datagram
(c) Header (d) None of these
17. Which is a connection oriented protocol?
- (a) TCP (b) SCTP
(c) UDP (d) None of these
18. Which is a situation in which too many sources over a network attempt to send data and the router buffers start overflowing due to which loss of packets occur?
- (a) Congestion (b) Error
(c) Event (d) None of these
19. Stream Control Transmission Protocol (SCTP) combines the features of which protocols?
- (a) TCP (b) UDP
(c) Both (a) and (b) (d) None of these

20. An endpoint of an inter-process communication flow across a computer network is called _____.
(a) socket (b) pipe
(c) port (d) None of these
21. User datagram protocol is called connectionless because _____.
(a) All UDP packets are treated independently by transport layer
(b) It sends data as a stream of related packets
(c) both (a) and (b)
(d) None of these
22. In the sending computer, UDP receives a data unit from the _____ layer.
(a) Application (b) Transport
(c) Network (d) None of these
23. UDP uses _____ to handle outgoing user datagrams from multiple processes on one host.
(a) flow control (b) multiplexing
(c) demultiplexing (d) None of these
24. The ports ranging from 49,152 to 65,535 can be used as temporary or private port numbers. They are called the _____ ports.
(a) well-known (b) registered
(c) dynamic (d) None of these
25. A port address in UDP is _____ bits long.
(a) 8 (b) 16
(c) 32 (d) None of these
26. TCP uses _____ to check the safe and sound arrival of data.
(a) an acknowledgment mechanism (b) out-of-band signaling
(c) the services of another protocol (d) None of these
27. UDP packets are encapsulated in _____.
(a) an Ethernet frame (b) an TCP segment
(c) an IP datagram (d) None of these
28. TCP has _____; SCTP has _____.
(a) packets; segments (b) segments; packets
(c) segments; frames (d) None of these
29. UDP uses _____ to handle incoming user datagrams that go to different processes on the same host.
(a) flow control (b) multiplexing
(c) demultiplexing (d) None of these

30. Communication in TCP is ____.
- | | |
|-----------------|-------------------|
| (a) simplex | (b) half-duplex |
| (c) full-duplex | (d) None of these |

ANSWERS

1. (d)	2. (c)	3. (b)	4. (a)	5. (c)	6. (d)	7. (c)
8. (a)	9. (c)	10. (b)	11. (d)	12. (c)	13. (b)	14. (c)
15. (d)	16. (a)	17. (a)	18. (a)	19. (c)	20. (a)	21. (a)
22. (a)	23. (b)	24. (c)	25. (b)	26. (a)	27. (c)	28. (b)
29. (c)	30. (c)					

Q. II Fill in the Blanks:

1. The _____ layer is responsible for error-free, end-to-end delivery of data from the source host to the destination host.
2. The transport layer provides a _____ control mechanism between the adjacent layers of the TCP/IP model.
3. A _____ is identified for each transport protocol and address combination by a 16-bits unsigned number, known as the port number.
4. A _____ is an application layer entity (running program) that uses the services of the transport layer.
5. Encapsulation happens at the _____ site.
6. If the producer delivers the items after the consumer has requested them, the delivery is referred to as _____.
7. Reliability can be achieved to add _____ control service to the transport layer.
8. When a packet is corrupted or lost, the receiving transport layer can somehow inform the sending transport layer to resend that packet using the _____ number.
9. The _____ is represented as a set of slices, called the sliding window, that occupy part of the circle at any time.
10. UDP is _____ protocol.
11. UDP packet called user _____.
12. TCP provides process-to-process communication using _____ numbers.
13. At the transport layer, TCP groups a number of bytes together into a packet called a _____.
14. To establish a connection, TCP uses a _____ handshaking.
15. In UDP, _____ are associated with ports.
16. UDP is a simple, unreliable transport protocol, which does not provide _____ and _____ control.

17. The _____ is one of the most important protocols of the Internet Protocols suite most widely used protocol for data transmission in communication networks such as the internet.
18. User Datagram Protocol (UDP) is a _____ layer protocol.
19. UDP _____ and connectionless protocol.
20. TCP is a _____ layer protocol that provides for a connection-oriented, reliable service to applications.
21. The combination of an IP address and a port number is called a _____ address.
22. A port number is a _____ address used to identify any client-server program uniquely.

ANSWERS

1. transport	2. flow	3. port	4. process	5. sender
6. pulling	7. error	8. sequence	9. buffer	10. stateless
11. datagram	12. port	13. segment	14. three-way	15. queues
16. error, flow	17. TCP	18. transport	19. unreliable	20. transport
21. socket	22. 16-bits			

Q. III State True or False:

1. The transport layer provides services such as connection-oriented communication, reliability, flow control, and multiplexing.
2. TCP also prevents data loss due to a fast sender and slow receiver by imposing some flow control techniques.
3. Error control uses open loop congestion control to prevent the congestion and closed loop congestion control to remove the congestion in a network once it occurred.
4. A process on the local host, called a client, needs services from a process usually on the remote host called a server.
5. Decapsulation happens at the receiver site.
6. If the sender delivers items whenever they are produced without the prior request from the consumer the delivery is referred to as pushing.
7. The error control service in transport layer, observes that the data delivered to the receiver is error free.
8. Congestion control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened.
9. In a connectionless oriented service, connection is established first and then data are transferred in between sender and receiver. After the end of data transfer, connection is released.

10. UDP provides a process to process communication using sockets, a combination of IP addresses and port numbers.
11. UDP provides checksums for data integrity, and port numbers for addressing different functions at the source and destination of the datagram.
12. UDP creates a virtual connection between two communicating entities/TCPs to send data.
13. Sequence numbers are 16 bit long that help identify which process is sending or receiving data on a host.
14. 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.
15. TCP uses two windows (send window and receive window) for each direction of data transfer.
16. In TCP, connection-oriented transmission requires three phases: connection establishment, data transfer, and connection termination.
17. To send a message from one process to another, the TCP protocol encapsulates and decapsulates messages in an IP datagram.
18. UDP services are Process to Process Communication, Connectionless Services, Flow Control, Error Control, Congestion Control, Encapsulation and Decapsulation, Queuing, Multiplexing and Demultiplexing.
19. UDP does not provide congestion control mechanisms.
20. Stream Control Transmission Protocol (SCTP) is a reliable, message-oriented transport layer protocol.
21. UDP does not guarantee ordered delivery of data.
22. TCP unreliable and connectionless protocol.
23. SCTP provides some of the features of both UDP and TCP, (it is message-oriented like UDP and ensures reliable, in-sequence transport of messages with congestion control like TCP).
24. A connection-oriented protocol establishes a connection, manages the data transfer and terminates the connection.

ANSWERS

1. (T)	2. (T)	3. (F)	4. (T)	5. (T)	6. (T)
7. (T)	8. (T)	9. (F)	10. (T)	11. (T)	12. (F)
13. (F)	14. (T)	15. (T)	16. (T)	17. (F)	18. (T)
19. (T)	20. (T)	21. (T)	22. (F)	23. (T)	24. (T)

Q. IV Answer the following Questions:**(A) Short Answer Questions:**

1. List functions of the transport layer.
2. What is the port number?
3. What is a socket address?
4. Define pulling.
5. What is a buffer?
6. Give role of sequence number.
7. Define congestion.
8. List transport layer protocols.
9. UDP is connectionless protocol. State true or false.
10. List UDP services.
11. What is TCP?
12. Which services are provided by TCP?

(B) Long Answer Questions:

1. Describe the process to process communication with diagrams.
2. Explain the following terms to transport layer:
 - (i) Multiplexing and demultiplexing.
 - (ii) Encapsulation and decapsulation.
3. With the help of diagram describe pushing and pulling in the transport layer.
4. Write a short note on: Sliding window.
5. Describe connectionless and connection-oriented services in detail.
6. What are the features of UDP?
7. Explain datagram format of UDP.
8. What are the services provided by UDP? Explain two of them in detail.
9. With the help of example, describe checksum.
10. Which services are provided by TCP?
11. With the help of diagram describe segment format of TCP.
12. Explain data transfer process of TCP with diagram.
13. Compare TCP and UDP.
14. Write a short note on: Windows in TCP.
15. Describe state transition diagram of TCP in detail.

UNIVERSITY QUESTIONS AND ANSWERS**April 2016**

1. Give header size of UDP packet. **[1 M]**

Ans. Refer to Section 4.3.2.

2. Write a short note on: UDP. **[5 M]**

Ans. Refer to Section 4.3.1.

April 2017

1. List any two features of TCP.

[1 M]

Ans. Refer to Section 4.4.2.

2. Explain the concept of multiplexing and demultiplexing used in process to process delivery.

[4 M]

Ans. Refer to Section 4.1.4.

October 2017

1. State any two applications of UDP.

[1 M]

Ans. Refer to Section 4.3.1.

2. Explain stream delivery service and sending and receiving buffer service of TCP.

[5 M]

Ans. Refer to Section 4.4.1, Point (2).

April 2018

1. What is the window size of the TCP segment?

[1 M]

Ans. Refer to Section 4.4.3.

2. Write a short note on: UDP.

[5 M]

Ans. Refer to Section 4.3.1.

3. Explain any four features supported by TCP.

[4 M]

Ans. Refer to Section 4.4.2.

October 2018

1. List the protocols used at the transport layer.

[1 M]

Ans. Refer to Section 4.3.

2. List the services provided by TCP.

[1 M]

Ans. Refer to Section 4.4.1.

3. Give difference between TCP and UDP.

[5 M]

Ans. Refer to Page No. 4.40.

April 2019

1. Draw and explain UDP datagram.

[5 M]

Ans. Refer to Section 4.3.2.

2. Explain TCP features.

[1 M]

Ans. Refer to Section 4.4.2.



NOTES



NOTES

