



**MAILAM**  
**Engineering College**

Approved by AICTE, New Delhi, affiliated to Anna University, Chennai, Accredited by NBA, NAAC & TCS

## **CS3591-COMPUTER NETWORKS**

**[REGULATION-2021]**

### **STUDY MATERIAL**

**DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND DATA SCIENCE**

**NAME OF THE STUDENT:.....**

**REGISTER NUMBER:.....**

**YEAR / SEM:.....**

**ACADEMIC YEAR:.....**

**PREPARED BY**

**Ms.V.Sankari,AP/AI&DS**



# MAILAM Engineering College

Approved by AICTE, New Delhi, affiliated to Anna University, Chennai, Accredited by NBA & TCS

## **DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND DATA SCIENCE**

### **CS3591 - COMPUTER NETWORKS**

**II Yr. / IV SEM**

### **SYLLABUS**

#### **COURSE OBJECTIVES:**

- To understand the concept of layering in networks.
- To know the functions of protocols of each layer of TCP/IP protocol suite.
- To visualize the end-to-end flow of information.
- To learn the functions of network layer and the various routing protocols
- To familiarize the functions and protocols of the Transport layer

#### **UNIT I      INTRODUCTION AND APPLICATION LAYER**

**10**

Data Communication - Networks – Network Types – Protocol Layering – TCP/IP Protocol suite – OSI Model – Introduction to Sockets - Application Layer protocols: HTTP – FTP – Email protocols (SMTP - POP3 - IMAP - MIME) – DNS – SNMP

#### **UNIT II      TRANSPORT LAYER**

**9**

Introduction - Transport-Layer Protocols: UDP – TCP: Connection Management – Flow control - Congestion Control - Congestion avoidance (DECbit, RED) – SCTP – Quality of Service

#### **UNIT III      NETWORK LAYER**

**7**

Switching : Packet Switching - Internet protocol - IPV4 – IP Addressing – Subnetting - IPV6, ARP, RARP, ICMP, DHCP

#### **UNIT IV      ROUTING**

**7**

Routing and protocols: Unicast routing - Distance Vector Routing - RIP - Link State Routing – OSPF – Path-vector routing - BGP - Multicast Routing: DVMRP – PIM.

**UNIT V DATA LINK AND PHYSICAL LAYERS****12**

Data Link Layer – Framing – Flow control – Error control – Data-Link Layer Protocols – HDLC – PPP - Media Access Control – Ethernet Basics – CSMA/CD – Virtual LAN – Wireless LAN (802.11) - Physical Layer: Data and Signals - Performance – Transmission media- Switching – Circuit Switching.

**45 PERIODS****COURSE OUTCOMES:**

At the end of this course, the students will be able to:

- CO 1: Explain the basic layers and its functions in computer networks.
- CO 2: Understand the basics of how data flows from one node to another.
- CO 3: Analyze routing algorithms.
- CO 4: Describe protocols for various functions in the network.
- CO 5: Analyze the working of various application layer protocols.

**TEXT BOOKS**

- 1. James F. Kurose, Keith W. Ross, Computer Networking, A Top-Down Approach Featuring the Internet, Eighth Edition, Pearson Education, 2021.
- 2. Behrouz A. Forouzan, Data Communications and Networking with TCP/IP Protocol Suite, Sixth Edition TMH, 2022

**REFERENCES**

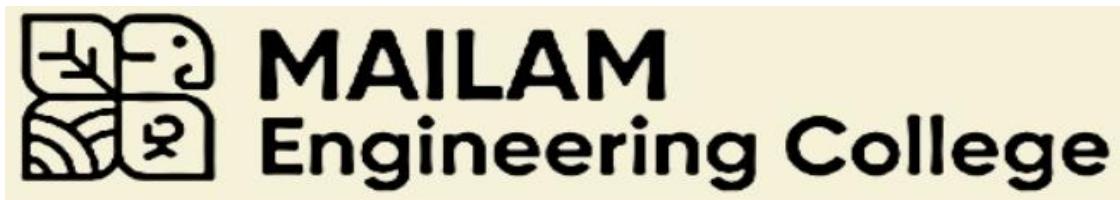
- 1. Larry L. Peterson, Bruce S. Davie, Computer Networks: A Systems Approach, Fifth Edition, Morgan Kaufmann Publishers Inc., 2012.
- 2. William Stallings, Data and Computer Communications, Tenth Edition, Pearson Education, 2013.
- 3. Nader F. Mir, Computer and Communication Networks, Second Edition, Prentice Hall, 2014.
- 4. Ying-Dar Lin, Ren-Hung Hwang, Fred Baker, "Computer Networks: An Open Source Approach", McGraw Hill, 2012.

**ANNA UNIVERSITY UPDATED QP – AP 2023, ND 2023, AP 2024, ND 2024**

**Prepared by –** *sankari*  
Mrs. V. Sankari, AP/AI&DS

**Verified By:** Dr. S. Artheeswari, HOD/AI&DS  
*S. Artheeswari 09/09/2025*

A handwritten signature in blue ink, followed by the word 'PRINCIPAL' in capital letters.



(Approved by AICTE, New Delhi, Affiliated to Anna University Chennai, Accredited by NBA, TCS & NAAC - 'A' Grade)

## **DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND DATA SCIENCE**

**II YEAR / IV SEM**

### **CS3591 – COMPUTER NETWORKS**

#### **SYLLABUS:**

#### **UNIT I INTRODUCTION AND APPLICATION LAYER**

Data Communication - Networks – Network Types – Protocol Layering – TCP/IP Protocol suite – OSI Model – Introduction to Sockets - Application Layer protocols: HTTP – FTP – Email protocols (SMTP - POP3 - IMAP - MIME) – DNS – SNMP.

#### **PART –A**

##### **1. Define network and computer network.(April/may 2023)**

A **network** is any **collection of independent computers** that communicate with one another over a shared network medium. A **computer network** is a **collection of two or more connected computers**. When these computers are joined in a network, people can share files and peripherals such as modems, printers, tape backup drives, or CD-ROM drives.

##### **2. List the Applications of Computer Network.**

###### **1. Business Applications**

- a. Database resource
- b. Communication Medium
- c. Electronic commerce

###### **2. Home Applications**

- a. Internet Access
- b. Personal Communication
- c. Entertainment
- d. Electronic Commerce

**3. Mobile Computers**

- a. Wireless networks

**3. What are the Advantages of Network?**

- **Speed.** Sharing and transferring files within Networks are very rapid. Thus saving time, while maintaining the integrity of the file.
- **Cost.** Individually licensed copies of many popular software programs can be costly. Networkable versions are available at considerable savings. Shared programs, on a network allows for easier upgrading of the program on one single file server, instead of upgrading individual workstations.
- **Security.** Sensitive files and programs on a network are password protected or designated as "copy inhibit," so that you do not have to worry about illegal copying of programs.
- **Centralized Software Management.** Software can be loaded on one computer (the file server) eliminating the need to spend time and energy installing updates and tracking files on independent computers throughout the building.
- **Resource Sharing.** Resources such as, printers, fax machines and modems can be shared.
- **Electronic Mail.** E-mail aids in personal and professional communication.
- **Flexible Access.** Access their files from computers throughout the firm.
- **Workgroup Computing.** Workgroup software (such as Microsoft BackOffice) allows many users to work on a document or project concurrently.

**4. What are the Disadvantages of Network?**

- Server faults stop applications being available.
- Network faults can cause loss of data.
- Network fault could lead to loss of resources.
- User work dependent upon network.
- Could become inefficient.
- Could degrade in performance.
- Resources could be located too far from users.

**5. What is a Point-to-Point type of connection?**

It provides a dedicated link between two devices of the channel. The entire capacity of the channel is reserved for transmission between those two devices.

**6. What is a multi type of connection?**

More than two devices can share a link by using this type of connection. It is also called as multidrop. The capacity channel is shared either temporary or spatially. If it simultaneously uses, it is spatially shared. If it takes turns, it is time shared line configuration.

**7. Define protocol layering.**

In data communication and networking, a protocol defines the rules that both the sender and receiver and all intermediate devices need to follow to be able to communicate effectively. When communication is simple, we may need only one simple protocol; when the communication is complex, we may need to divide the task between different layers, in which case we need a protocol at each layer, or **protocol layering**.

**8. What are the major duties of network layer? (MAY 2012)**

- **Logical addressing** - If a packet passes the n/w boundary, we need another addressing system for source and destination called logical address.
- **Routing** – The devices which connects various networks called routers are responsible for delivering packets to final destination.

**9. What are the functions of application layer? (MAY 2011)**

- **FTAM (file transfer, access, mgmt)** - Allows user to access files in a remote host.
- **Mail services** - Provides email forwarding and storage.
- **Directory services** - Provides database sources to access information about various sources and objects.

**10. Define a layer. (Nov/Dec 2013)**

The OSI (Open System Interconnection) Model **breaks the various aspects of a computer network into seven distinct layers**. Each successive layer envelopes the layer beneath it, hiding its details from the levels above.

**11. What do you mean by framing? (Nov/Dec 2013) (Nov/Dec 2014)****Frames are the small data units**

Created by data link layer and the process of creating frames by the data link layer is known as framing.

**12. What is protocol? What are its key elements? (NOV/DEC 2007) &(May 2016).**

Set of rules that govern the data communication is protocol. The key elements are,

- i) Syntax.
- ii) Semantics.
- iii) Timing.

**13. List the 7 OSI layers.**

- Physical Layer.
- Data link Layer.
- Network Layer.
- Transport Layer.
- Session Layer.
- Presentation Layer.
- Application Layer.

**14. Define the terms: Bandwidth & Latency (Dec 2017).**

Network performance was measured in two fundamental ways: **bandwidth** (also called *throughput*) and **latency** (also called *delay*).

- The bandwidth of a network is given by the **number of bits that can be transmitted over the network in a certain period of time.**
- The second performance metric, latency, corresponds to **how long it takes a message to travel from one end of a network to the other.**

**15. List the requirements to building a network.**

- ✓ Scalable Connectivity.
- ✓ Cost-Effective Resource Sharing.
- ✓ Support for Common Services.
- ✓ Manageability.

**16. Write the parameters used to measure network performance.(May 2016).**

- Bandwidth and Latency.
- Delay×Bandwidth Product.
- High-Speed Networks.
- Application Performance Needs.

**17. What are the three criteria necessary for an effective and efficient network?**

The most important criteria are

- ✓ Performance
- ✓ Reliability
- ✓ Security

1. **Performance** of the network depends on number of users, type of transmission medium, and the capabilities of the connected h/w and the efficiency of the s/w.
2. **Reliability** is measured by frequency of failure, the time it takes a link to recover from the failure and the network's robustness in a catastrophe.
3. **Security** issues include protecting data from unauthorized access and viruses.

**18. Group the OSI layers by function. (Nov/Dec 2020).**

The seven layers of the OSI model belonging to three subgroups. Physical, data link and network layers are the **network support layers**; they deal with the physical aspects of moving data from one device to another. Session, presentation and application layers are the **user support layers**; they allow interoperability among unrelated software systems. The transport layer ensures **end-to-end reliable data transmission.**

**19. What are the features provided by layering? (May 2013).**

Two features:

- It **decomposes the problem** of building a network into more manageable components.
- It provides a more **modular design**.

**20. Why are protocols needed?**

In networks, communication occurs between the entities in different systems. Two entities cannot just send bit streams to each other and expect to be understood. For communication, the entities must agree on a protocol. **A protocol is a set of rules that govern data communication.**

**21. Explain the two types of duplex.**

- **Full duplex**-two bit streams can be simultaneously transmitted over the links at the same time, one going in each direction.
- **Half duplex**-it supports data flowing in only one direction at a time.

**22. What are the responsibilities of data link layer?**

Specific responsibilities of data link layer include the following.

- a) Framing.
- b) Physical addressing.
- c) Flow control.
- d) Error control.
- e) Access control.

**23. Define flow control. (NOV 2011)(May 2015) (May 2016).**

Flow control refers to a set of procedures used to restrict the amount of data.  
The sender can send before waiting for acknowledgment.

**24. Mention the categories of flow control.**

There are 2 methods have been developed to control flow of data across communication links.

- a) Stop and wait - send one frame at a time.
- b) Sliding window - send several frames at a time.

**25. What is a buffer?**

Each receiving device has a block of memory called a buffer, reserved for storing incoming data until they are processed.

**26. What is HTTP?****HTTP PROTOCOL (Hyper Text Transfer Protocol)**

- Protocol for transfer of data between Web servers and Web clients (browsers).
- “The Hypertext Transfer Protocol (HTTP) is an **application-level protocol** for **distributed**, collaborative, hypermedia information systems.
- **Popular Web servers:**
  - Apache HTTPD, JBoss and Tomcat.
- **Popular Web clients:** Firefox and Opera.

**27. What is FTP?**

FTP (**File Transfer Protocol**) is a network protocol for transmitting files between computers over Transmission Control Protocol/Internet Protocol (TCP/IP) connections. Within the TCP/IP suite, FTP is considered an application layer protocol.

**28. What is SMTP?**

The TCP/IP protocol supports electronic mail on the Internet is called Simple Mail Transfer (SMTP). It is a system for sending messages to other computer users based on e-mail addresses. SMTP provides mail exchange between users on the same or different computers.

**29. What is POP3?(april/may 2023)**

POP3 (**Post Office Protocol 3**) is the most recent version of a standard protocol for receiving e-mail. POP3 is a **client/server protocol** in which e-mail is received and held for you by your Internet server. POP and IMAP deal with the receiving of e-mail and are not to be confused with the Simple Mail Transfer Protocol (**SMTP**), a protocol for transferring e-mail across the Internet.

**30. What is IMAP?**

IMAP (**Internet Message Access Protocol**) is a standard **protocol** for accessing **e-mail** from your local server. IMAP (**the latest version is IMAP Version 4**) is a **client/server** protocol in which e-mail is received and held for you by your Internet server. IMAP can be thought of as a remote file server. POP3 can be thought of as a "store-and-forward" service.

**31. What is MIME?**

MIME, an acronym for **Multipurpose Internet Mail Extensions**, **specifies how messages must be formatted so that they can be exchanged between different email systems**. MIME is a very flexible format, permitting one to include virtually any type of file or document in an email message. MIME messages can contain text, images, audio, video, or other application-specific data.

**32. Define DNS.**

The **DNS** translates Internet domain and host names to **IP addresses**. DNS automatically converts the names we type in our Web browser address bar to the IP addresses of Web servers hosting those sites.

**33. Why name services are sometimes called as middleware?**

Name services are sometimes called middleware because **they fill a gap between applications and the underlying network.**

**34. What are the types of DNS message?**

Two types of messages

- Query: header and question records.
- Response: Header, question records, answer records, authoritative records, and additional records.

**35. Define SNMP.**

- SNMP is a frame work for managing devices in an internet using TCP/IP suite.
- It provides fundamental operations for monitoring and maintaining an internet.

**36. What are the two mainly used application protocols?**

- Simple Mail Transfer Protocol (SMTP) is used to exchange electronic mail.
- Hypertext Transport Protocol (HTTP) is used to communicate between web browsers and web servers.

**37. What are the groups of HTTP header? (May 2015)**

- Accept
- HTTP\_User-Agent
- Content-Language
- Content-Length
- Content-Type
- Date
- Expires:
- Host
- Location
- Retry-After

**38. Mention the types of HTTP messages.**

- HTTP request message
- HTTP response message

**39. State the usage of conditional get in HTTP. (Apr/May 2017)**

A conditional GET is an HTTP GET request that may return an HTTP 304 response (instead of HTTP 200). An HTTP 304 response indicates that the resource has not been modified since the previous GET, and so the resource is not returned to the client in such a response.

**40. Define URL. (May 2016)**

- A URL (Uniform Resource Locator), as the name suggests, provides a way to locate a resource on the web, the hypertext system that operates over the internet. The URL contains the name of the protocol to be used to access the resource and a resource name. The first part of a URL identifies what protocol to use. The second part identifies the IP address or domain name where the resource is located.

**41. Write the use of HTTP. (Apr-May 2017)**

**HTTP (Hypertext Transfer Protocol)** is the set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. As soon as a Web user opens their Web browser, the user is indirectly making use of HTTP. HTTP is an application protocol that runs on top of the TCP/IP suite of protocols (the foundation protocols for the Internet).

**42. What is persistent HTTP? What are the advantages of allowing persistent****TCP Connections in HTTP? (May 2013) & (Nov 2016)**

HTTP persistent connection, also called HTTP keep-alive, or HTTP connection reuse, is the idea of using a single TCP connection to send and receive multiple HTTP requests/responses, as opposed to opening a new connection for every single request/response pair.

**43. Define socket. (April/may 2024)**

- A **socket** is one endpoint of a two way communication link between two programs running on the network.
- The socket mechanism provides a means of inter-process communication (IPC) by establishing named contact points between which the communication take place.

**44. What are the functionalities of SNMP protocol?(April/may 2024)**

- SNMP enables administrators to monitor how devices are performing and make changes to network devices so that data moves through the network more efficiently.
- SNMP collects, organizes, and sends data from various devices for network monitoring assisting with fault identification and isolation.

**45. What are the basic task of communication system?(Nov/Dec 2023)**

The transmitter's function is to process the message signal into a form suitable for transmission over the communication channel. This is called modulation. As for the communication channel, its function is to provide a pathway between the transmitter's output and the receiver's input.

**46. What is the meaning of stateful and stateless of a protocol? Give an example for each one?(Nov/Dec 2023)**

A Stateful Protocol is a type of network protocol in which the client sends a server request and expects some sort of response. In case it doesn't get a response, it then resends the intended request.

**Example:**Telnet, File Transfer Protocol (FTP), etc.

**PART-B**

**1.Explain in details about the data communication with suitable diagram.**

**Synopsis:**

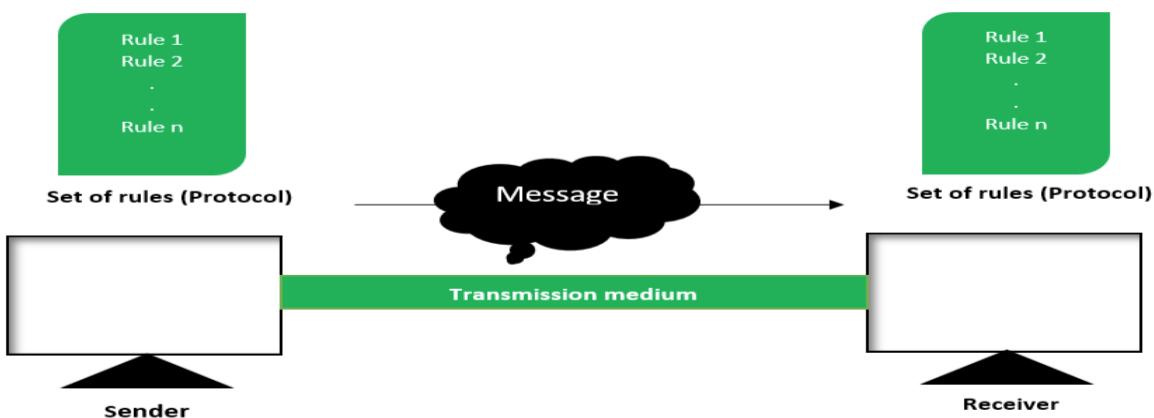
- |                                  |
|----------------------------------|
| <b>1.1 DATA COMMUNICATIONS</b>   |
| <b>1.1.1 Components</b>          |
| <b>1.1.2 Data Representation</b> |
| <b>1.1.3 Data Flow</b>           |

### **1.1 DATA COMMUNICATIONS**

- Data communications are the **exchange of data between two devices** via some form of transmission medium such as a wire cable.
- The effectiveness of a data communications system depends on four fundamental characteristics:
  - **Delivery:** The system must deliver data to the correct destination.
  - **Accuracy:** The system must deliver the data accurately
  - **Timeliness:** The system must deliver data in a timely manner.
  - **Jitter:** Jitter refers to the variation in the packet arrival time.

#### **1.1.1 Components**

Fig:1.1 Shows the components of data communication systems



**Fig.1.1 Data communication components**

#### **Message:**

- The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.

**Sender:**

- The sender is the device that sends the data message.
- It can be a computer, workstation, telephone handset, video camera, and so on.

**Receiver:**

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

**Transmission medium.**

- The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.

**Protocol.**

- A protocol is a set of rules that govern data communications.

**1.1.2 Data Representation**

Information today comes in different forms such as **text, numbers, images, audio, and Video.**

**Text:** Text is represented as a bit pattern, a sequence of bits.

**Numbers:** Numbers are also represented by bit patterns. However, a code such as ASCII is not used to represent numbers.

**Images:** Images are also represented by bit patterns. In its simplest form, an image is composed of a matrix of pixels (picture elements), where each pixel is a small dot.

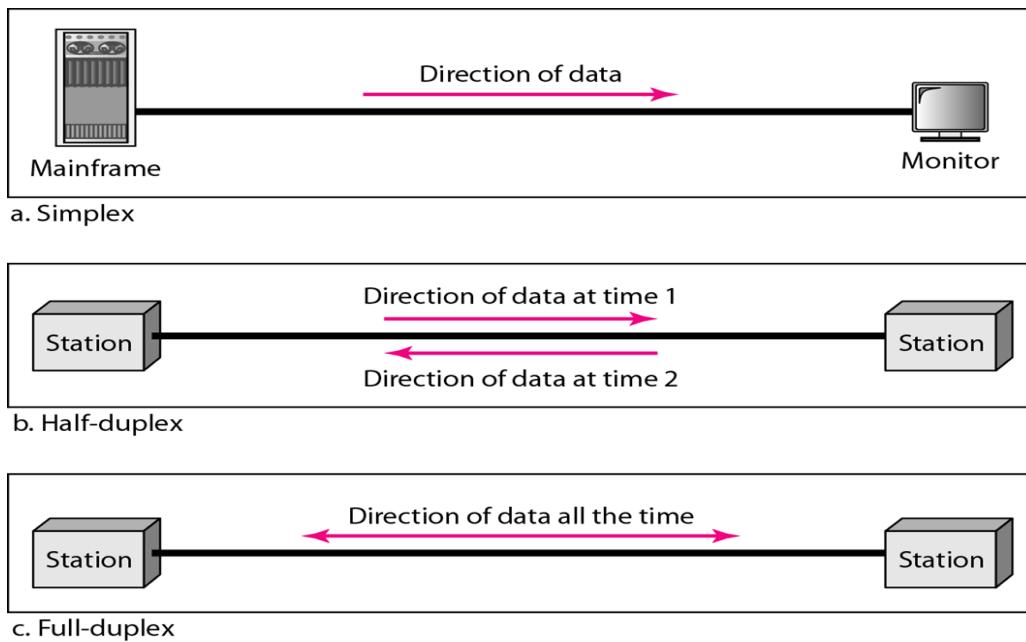
**Audio:** Audio refers to the recording or broadcasting of sound or music.

Audio is by nature different from text, numbers, or images. It is continuous, not discrete.

**Video:** Video refers to the recording or broadcasting of a picture or movie.

**1.1.3 Data Flow**

Communication between two devices can be simplex, half-duplex, or full-duplex as Shown in Figure 1.2.

**Figure.1.2 Data Flow**

**Simplex:** In simplex mode, the communication is unidirectional, as on a one way street.

Only one of the two devices on a link can transmit; the other can only receive. (see Figure 1.2a).

### **Half-Duplex**

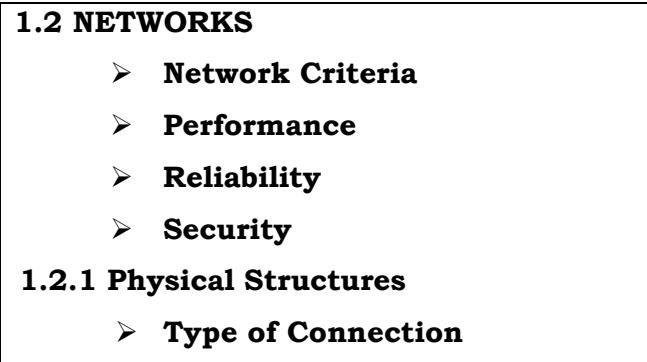
- In half-duplex mode, each station can both transmit and receive, but not at the same time.
- When one device is sending, the other can only receive, and vice versa. (see Figure 1.2b).

### **Full-Duplex**

- In full-duplex (also@ called duplex), both stations can transmit and receive simultaneously.(see Figure 1.2c).

## **2.Explain in details about the networks with suitable diagram.**

### **Synopsis:**



## **1.2 NETWORKS**

A network is a set of devices (often referred to as *nodes*) connected by communication links. 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.

### **Network Criteria**

A network must be able to meet a certain number of criteria. The most important of these are **performance, reliability, and security**.

#### **Performance**

- Performance can be measured in many ways, **including transit time and response time**.
- **Transit time** is the amount of time required for a message to travel from one device to another.
- **Response time** is the elapsed time between an inquiry and a response.

#### **Reliability**

In addition to accuracy of delivery, network reliability is measured by the frequency of Failure.

#### **Security**

Network security issues include protecting data from unauthorized access, protecting data from damage and development.

## **1.2.1 Physical Structures**

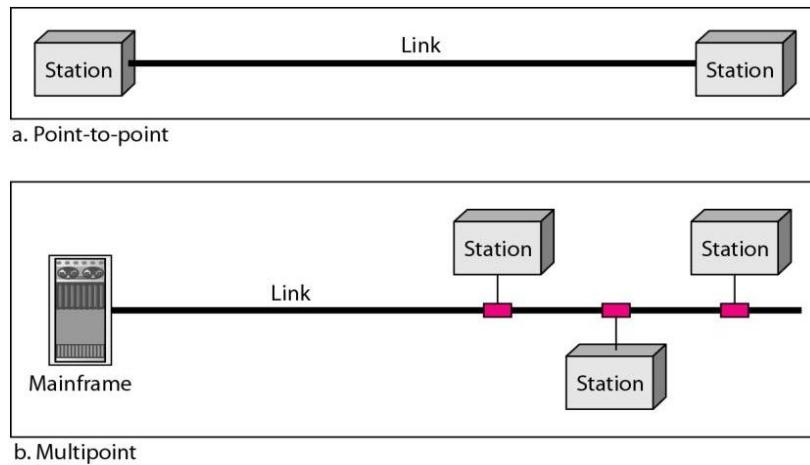
### **Type of Connection**

A link is a communications pathway that transfers data from one device to another.

- Point-to-Point
- Multipoint

**Point-to-Point:** A point-to-point connection provides a dedicated link between two devices. (see Figure 1.3a).

**Multipoint:** A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link (see Figure 1.3b).



**Figure 1.3 Types of connections: point-to-point and multipoint**

**3.Explain in details about the networks types with suitable diagram.**

**Synopsis:**

### 1.3 Categories of Networks

- Local-area networks
- Metropolitan area networks
- Wide-area networks

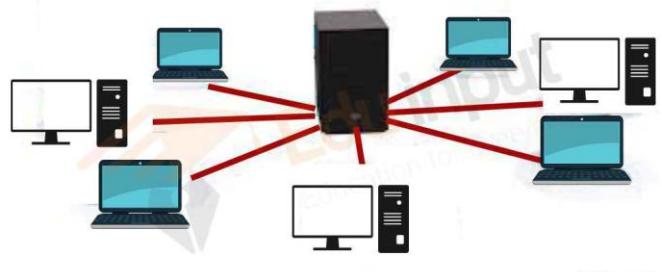
### 1.3 Categories of Networks

- Local-area networks
- Metropolitan area networks
- Wide-area networks

### Local Area Network

A local area network (LAN) is usually privately owned and links the devices in a single office, building, or campus (see Figure 1.4).

### **Local Area Network (LAN)**

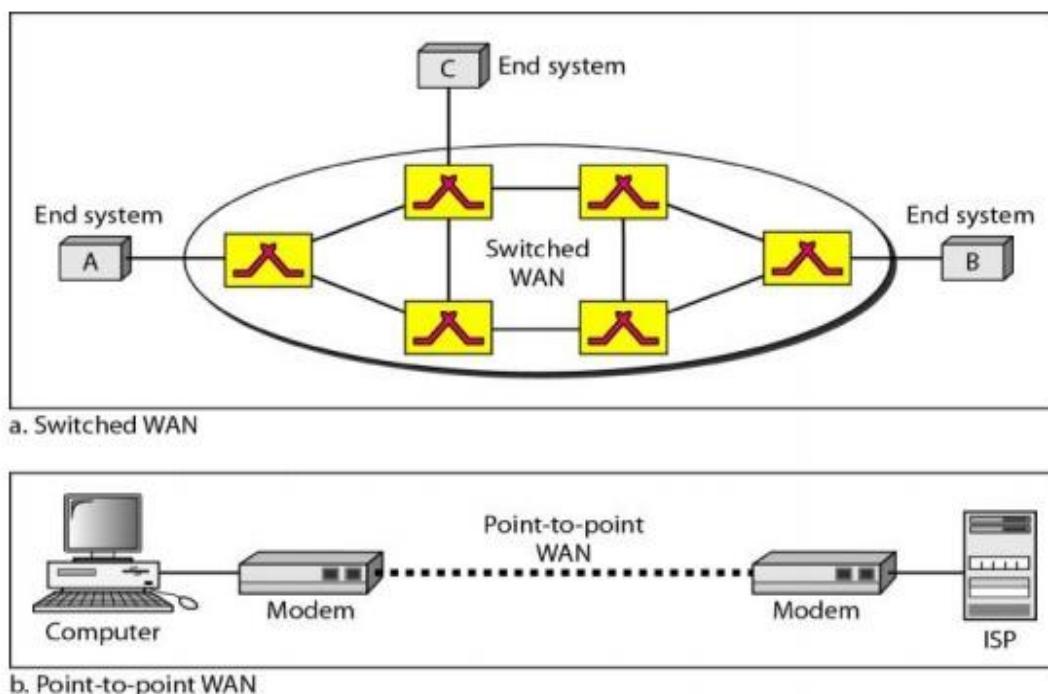


**Figure 1.4. Local Area Network**

- 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.
- A common example of a LAN, found in many business environments, links a workgroup of task-related computers, for example, engineering workstations or accounting PCs.

### **Wide Area Network**

A wide area network (WAN) provides **long-distance transmission of data**, image, audio, and video information over large geographic areas that may comprise a country, a continent, or even the whole world. (see Figure 1.5).



**Figure 1.5 Wide Area Network**

### **Metropolitan Area Networks**

A metropolitan area network (MAN) is a network with a size between a LAN and a WAN. It normally covers the area inside a town or a city.

### **Internet**

An internet (**note the lowercase letter i**) is two or more networks that can communicate with each other. (An internet is a network of networks)

### **Internet**

The most notable internet is called the Internet (**uppercase letter I**), a collaboration of more than hundreds of thousands of interconnected networks.

(The Internet is a collection of many separate networks.)

### **Topology**

Topology refers to the physical or logical arrangement of a network. Devices may be arranged in a mesh, star, bus, or ring topology.

### **Protocol**

A protocol is a set of rules that govern data communication; the key elements of a protocol are syntax, semantics, and timing.

**4.Explain in details about the OSI MODEL with suitable diagram.(April/may 2024)/April/may 2023**

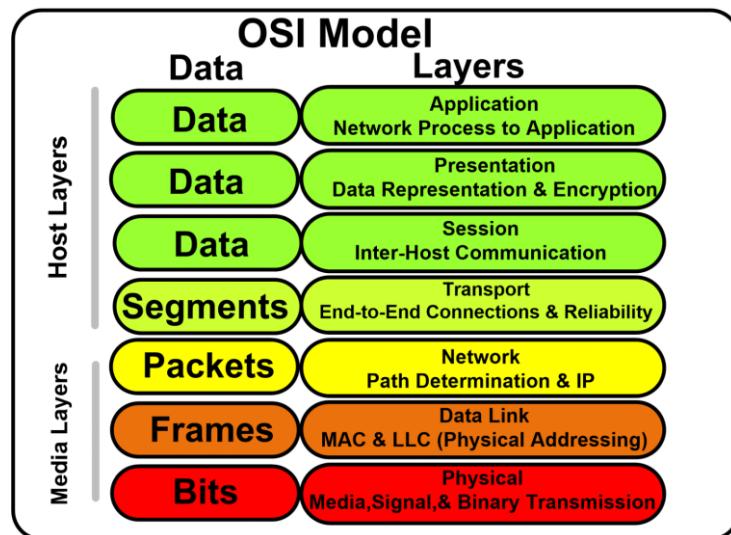
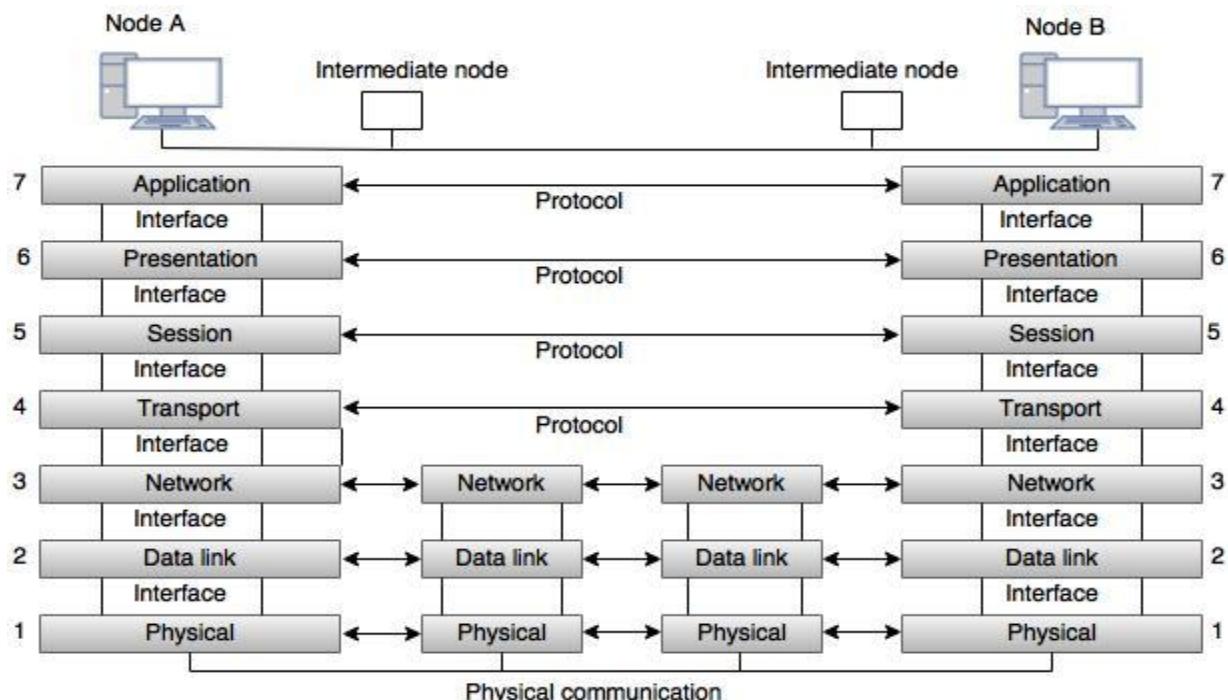
**Synopsis:**

- |  |
|--|
| <p><b>1.4 THE OSI MODEL</b></p> <p><b>Definition</b></p> <p><b>1.4.1 TYPES OF OSI MODEL</b></p> <ul style="list-style-type: none"><li><b>1. Physical Layer.</b></li><li><b>2. Data Link Layer.</b></li><li><b>3. Network Layer.</b></li><li><b>4. Transport Layer.</b></li><li><b>5. Session Layer.</b></li><li><b>6. Presentation Layer.</b></li><li><b>7. Application Layer.</b></li></ul> |
|--|

### **1.4 THE OSI MODEL**

- The OSI model is not a protocol; it is a model for **understanding and designing a network** architecture that is flexible, robust, and interoperable. (see Figure 1.6).
- It was developed by ISO.

**ISO is the organization. OSI is the model**

**Figure 1.6 seven layers of the OSI model****Fig: OSI Model****Figure: 1.7 The interaction between layers in the OSI model**

- At the physical layer, communication is direct: In Figure 1.7, device A sends a stream of bits to device B (through intermediate nodes). At the higher layers, however, communication must move down through the layers on device A, over to device B, and then back up through the layers.

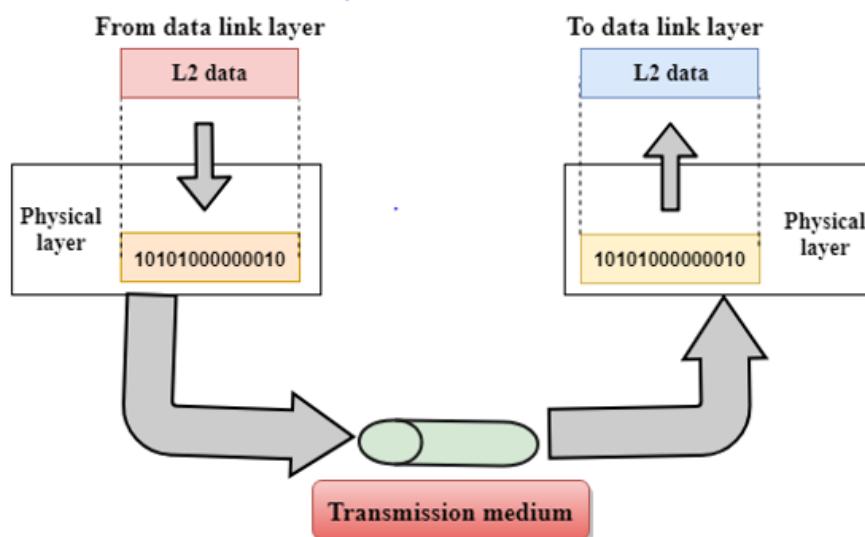
### **1.4.1 TYPES OF OSI MODEL:**

- There are seven layers in the OSI model,
  1. Physical Layer.
  2. Data Link Layer.
  3. Network Layer.
  4. Transport Layer.
  5. Session Layer.
  6. Presentation Layer.
  7. Application Layer.

#### **Physical Layer**

- The physical layer coordinates the functions required to carry a bit stream over a physical medium.
- It deals with the mechanical and electrical specifications of the interface and transmission medium.
- Figure 1.8 shows the position of the physical layer with respect to the transmission medium and the data link layer.

**The physical layer is responsible for movements of individual bits from one hop (node) to the next.**



**Figure 1.8 Physical layer.**

The physical layer is also concerned with the following:

**Physical characteristics of interfaces and medium.**

- The 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.**

- The physical layer data consists of a stream of bits (sequence of Os or 1s) with no interpretation. To be transmitted, bits must be encoded into signals--electrical or optical. The physical layer defines the type of encoding (how Os and 1s are changed to signals).

**Data rate.** The transmission rate-the number of bits sent each second-is also defined by the physical layer.

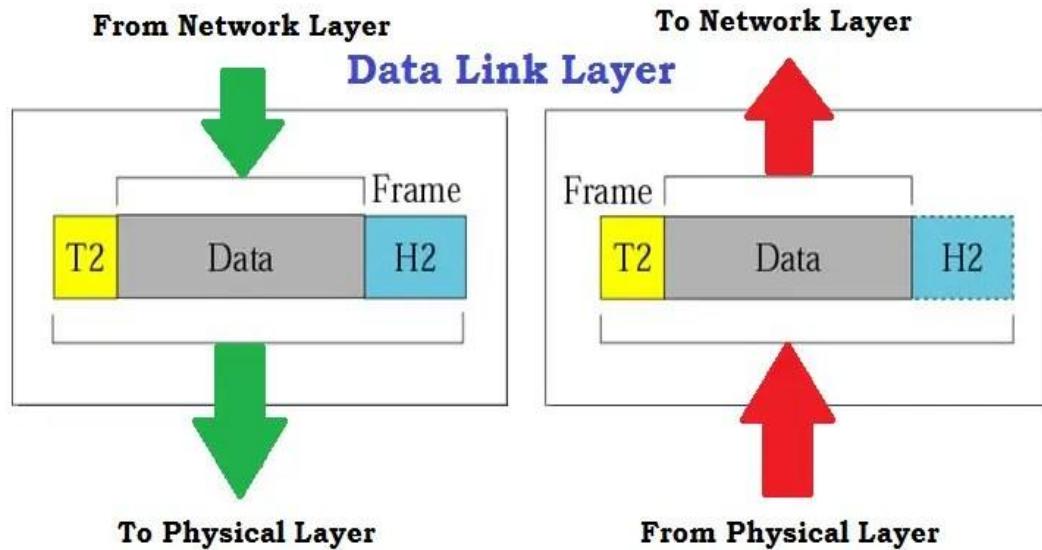
**Synchronization of bits.** The sender and receiver not only must use the same bit rate but also must be synchronized at the bit level.

**Line configuration.** The physical layer is concerned with the connection of devices to the media. In a point-to-point configuration, two devices are connected through a dedicated link. In a multipoint configuration, a link is shared among several devices.

**Transmission mode.** The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex. In simplex mode, only one device can send; the other can only receive. The simplex mode is a one-way communication. In the half-duplex mode, two devices can send and receive, but not at the same time. In a full-duplex (or simply duplex) mode, two devices can send and receive at the same time.

**Data Link Layer**

- The data link layer transforms the physical layer, a raw transmission facility, to a reliable link.
- It makes the physical layer appear error-free to the upper layer (network layer). Figure 1.9 shows the relationship of the data link layer to the network and physical layers.

**Figure 1.9 Data link layer**

**The data link layer is responsible for moving frames from one hop (node) to the next.**

**Other responsibilities of the data link layer include the following:**

**Framing:**

- The data link layer divides the stream of bits received from the network layer into manageable data units called frames.

**Physical addressing:**

- If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame.
- If the frame is intended for a system outside the sender's network, the receiver address is the address of the device that connects the network to the next one.

**Flow control:**

- If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.

**Error control:**

- The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames.
- Error control is normally achieved through a trailer added to the end of the frame.

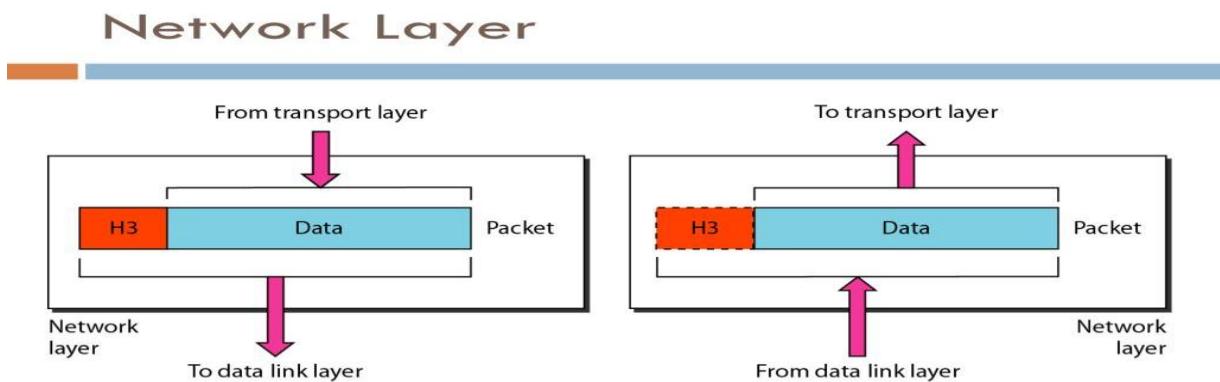
**Access control:**

- When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.

**Network Layer**

- The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links).

Figure 1.10 shows the relationship of the network layer to the data link and transport layers.



**Figure 1.10 Network layer**

**The network layer is responsible for the delivery of individual packets from the source host to the destination host.**

**Other responsibilities of the network layer include the following:**

**Logical addressing**

The physical addressing implemented by the data link layer handles the addressing problem locally. If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. The network layer adds a

header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver.

### **Routing.**

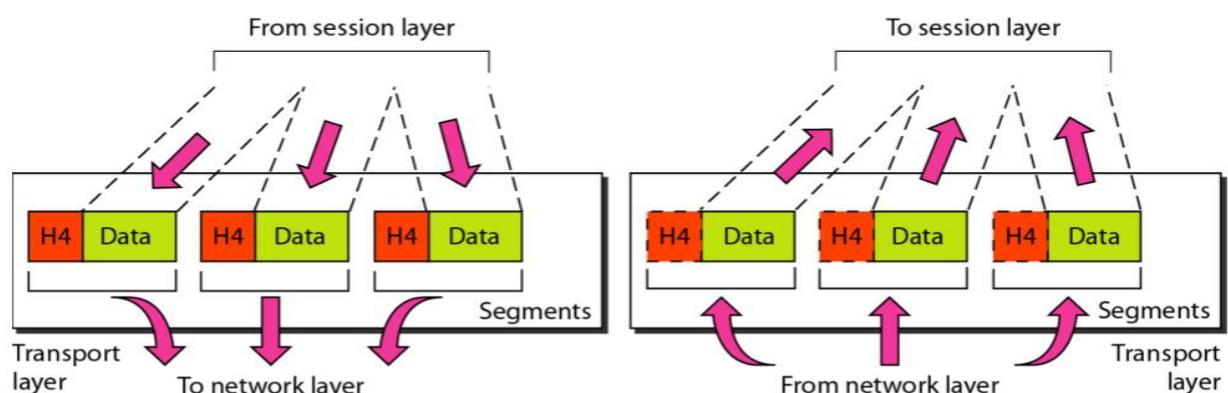
When independent networks or links are connected to create *internetworks* (network of networks) or a large network, the connecting devices (called *routers* or *switches*) route or switch the packets to their final destination.

### **Transport Layer**

The transport layer is responsible for process-to-process delivery of the entire message.

Figure 1.11 shows the relationship of the transport layer to the network and session layers.

## **Transport Layer**



**Figure 1.11 Transport layers**

**The transport layer is responsible for the delivery of a message from one process to another**

**Other responsibilities of the transport layer include the following:**

- Service-point addressing.
- Segmentation and reassembly.
- Connection control.
- Flow control.
- Error control.

### **Session Layer**

- The session layer is the network ***dialog controller***.
- It establishes, maintains, and synchronizes the interaction among communicating Systems.

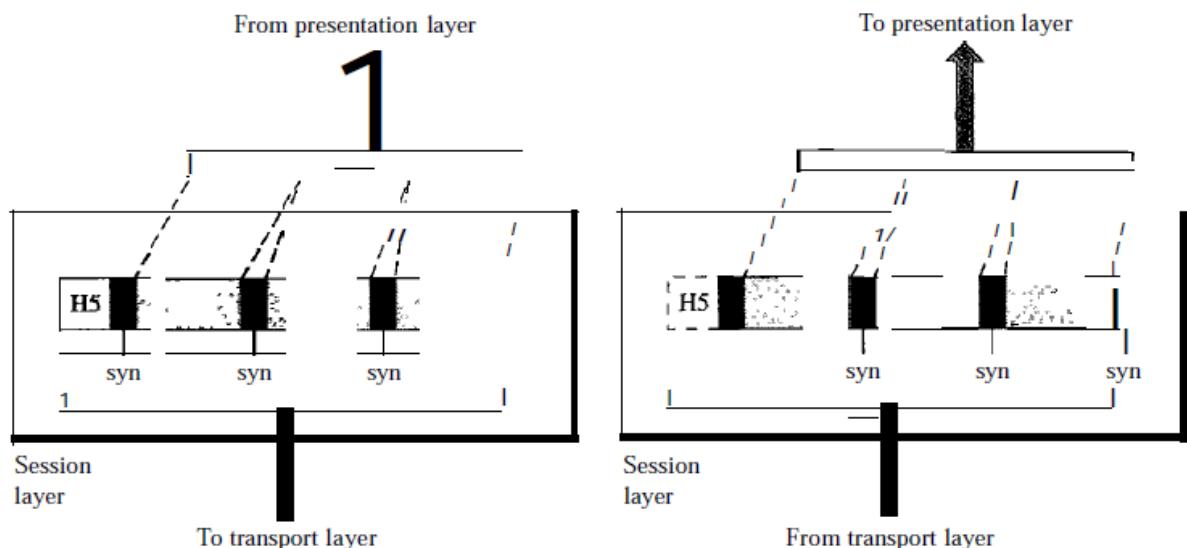
**The session layer is responsible for dialog control and synchronization**

### **Specific responsibilities of the session layer include the following:**

- Dialog control.
- Synchronization.

### **Presentation Layer**

- The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems. Figure 1.12 shows the relationship between the presentation layer and the application and session layers.



**Figure 1.12 Presentation Layer**

### **Specific responsibilities of the presentation layer include the following:**

#### **Translation:**

- The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers, and so on.

#### **Encryption:**

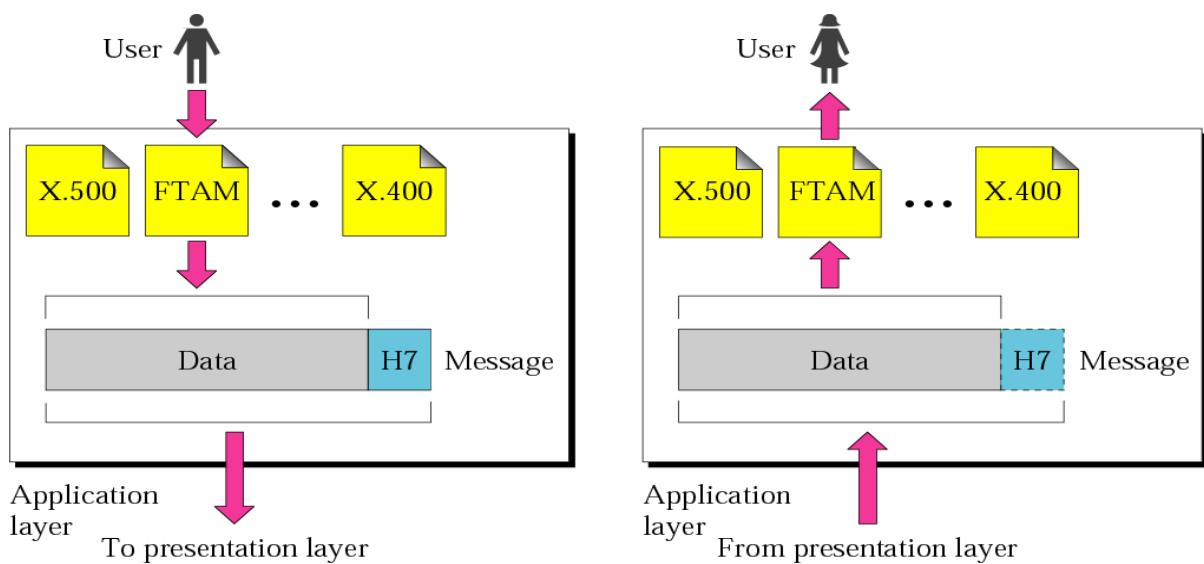
- Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network.

**Compression:**

- Data compression reduces the number of bits contained in the information.

**Application Layer**

- The application layer enables the user, whether human or software, to access the network.
- It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.
- Figure 1.13 shows the relationship of the application layer to the user and the presentation layer.

**Figure 1.13 Application layer**

The application layer is responsible for providing services to the user

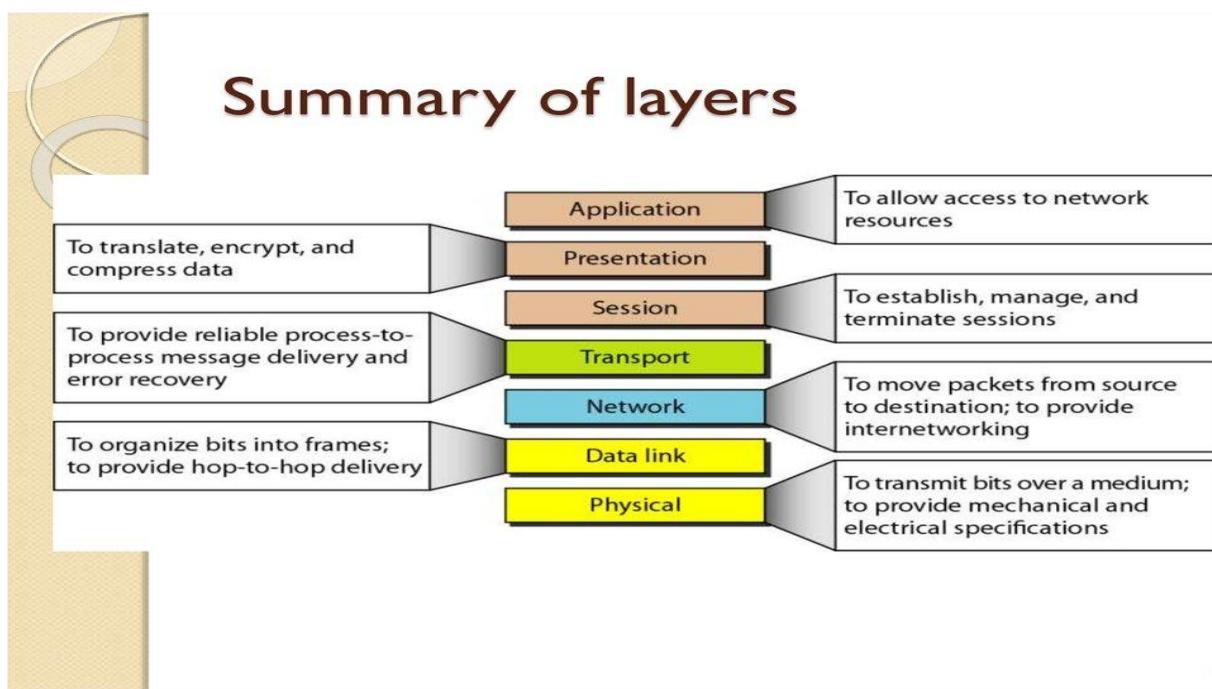
**Specific services provided by the application layer include the following:****Network virtual terminal:**

- A network virtual terminal is a software version of a phys File transfer, access, and management.
- This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally terminal, and it allows a user to log on to a remote host.

**Mail services:**

- This application provides the basis for e-mail forwarding and storage.

Figure 1.14 shows a summary of duties for each layer.



2.29

**Figure 1.14 Summary of layers**

**5. Explain in details about the TCP/IP PROTOCOL with suitable diagram.(Nov/dec 2023)**

**Synopsis:**

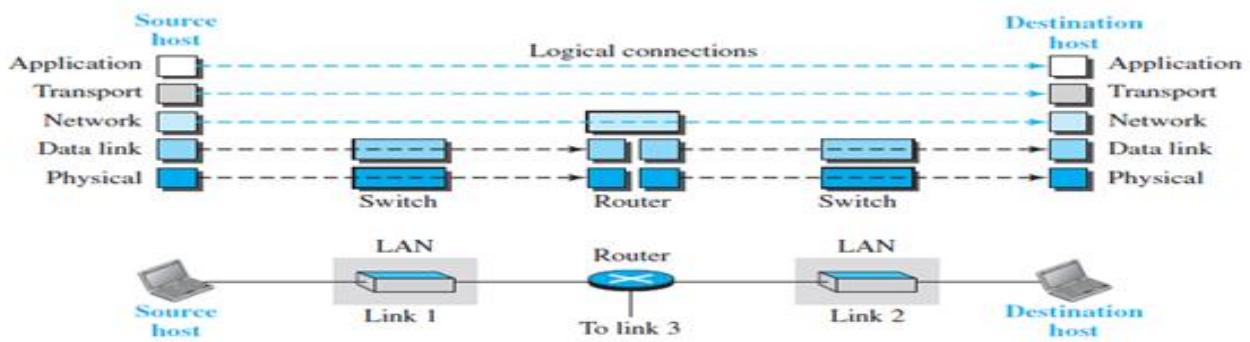
- |   |
|---|
| <b>1TCP/IP ARCHITECTURE</b>   |
| <ul style="list-style-type: none"> <li>• <b>Network Interface Layer</b></li> <li>• <b>Internet Layer</b></li> <li>• <b>Transport (also known as Host-to-Host or Transmission) Layer.</b></li> <li>• <b>Application Layer (known earlier as the Process Layer).</b></li> </ul> |

**1.5. TCP/IP ARCHITECTURE**

TCP/IP model is an implementation of OSI reference model. It has four layers. They are,

- Network Interface Layer
- Internet Layer
- Transport (also known as Host-to-Host or Transmission) Layer

- Application Layer (known earlier as the Process Layer) (see Figure 1.15).



**Fig 1.15 – Logical connection between layers**

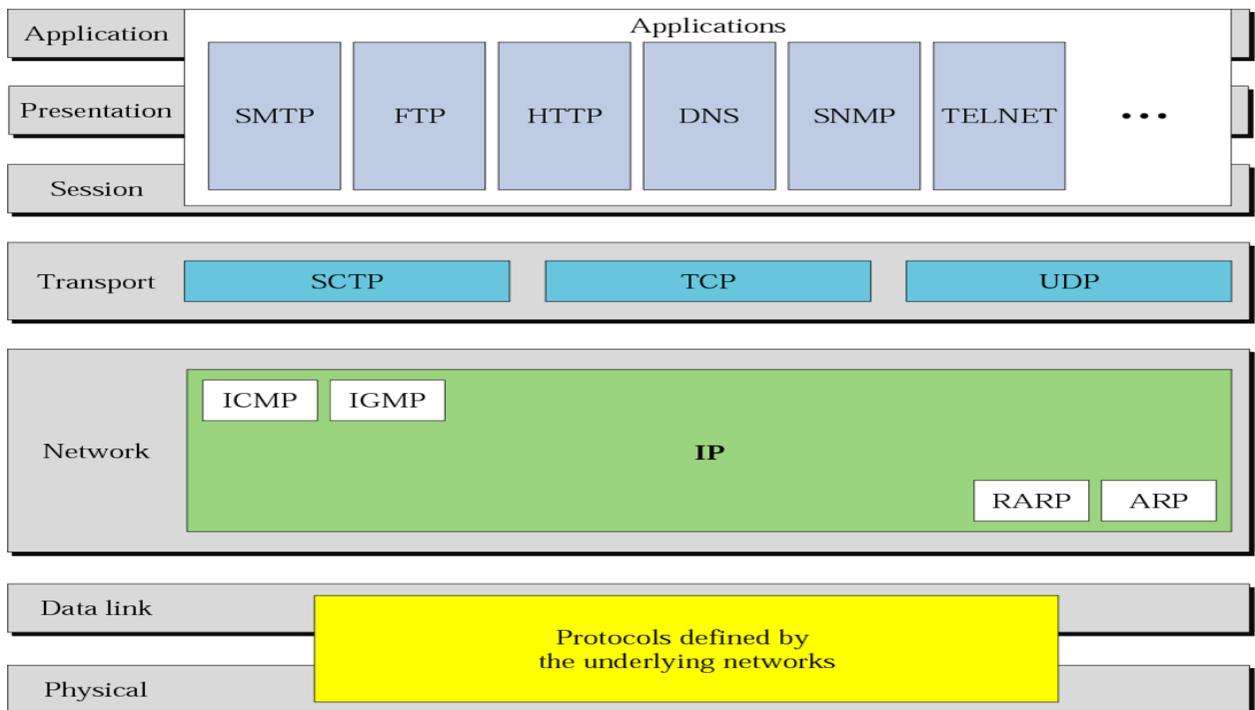
- The TCPIIP protocol suite was developed prior to the OSI model.
- The original TCP/IP protocol suite was defined as having four layers: host-to-network, internet, transport, and application.

The first four layers provide,

- Physical standards,
- Network interfaces,
- Internetworking,
- And transport functions
  - That correspond to the first four layers of the OSI model. The three topmost layers in the OSI model, however, are represented in TCPIIP by a single layer called the **application layer** (see Figure 1.16).

**At the transport layer, TCP/IP defines three protocols:**

- Transmission Control Protocol (TCP),
- User Datagram Protocol (UDP), and
- Stream Control Transmission Protocol (SCTP).
- At the network layer, the main protocol defined by TCP/IP is the Internetworking Protocol (IP); there are also some other protocols that support data movement in this layer.



**Figure 1.16 TCP/ IP and OSI model**

### **1) Network interface layer (or) The Host to Network Layer:**

Below the internet layer is great void. The TCP/IP reference model does not really say such about what happen here, except to point out that **the host has connect to the network using some protocol so it can transmit IP packets over it**. This protocol is not specified and varies from host to host and network to network.

### **2) Internet layer:**

Packet switching network depends upon a connectionless internetwork layer. This layer is known as internet layer, is the linchpin that holds the whole design together. Its job is to **allow hosts to insert packets into any network and have them to deliver independently to the destination**. They may appear in a different order than they were sent in each case it is job of higher layers to rearrange them in order to deliver them to proper destination.

The internet layer specifies an official packet format and protocol known as internet protocol. **The job of internet layer is to transport IP packets to appropriate destination**. Packet routing is very essential task in order to avoid congestion. For these reason it is say that TCP/IP internet layer perform same function as that of OSI network layer.

### **3) Transport layer:**

- In the TCP/IP model, the layer above the internet layer is known as transport layer. It is **developed to permit entities on the source and destination**

**hosts to carry on a conversation.** It specifies 2 end-to-end protocols (Refer fig 1.5 a)

- i. TCP (Transmission Control Protocol)
- ii. UDP (User Datagram Protocol)

### **TCP**

- It is a **reliable connection-oriented protocol** that permits a byte stream originating on one machine to be transported without error on any machine in the internet.
- It divides the incoming byte stream into discrete message and passes each one onto the internet layer.
- At the destination, the receiving TCP process collects the received message into the output stream.
- TCP deals with flow control to make sure a fast sender cannot swamp a slow receiver with more message than it can handle.

### **UDP**

- It is an **unreliable, connectionless protocol** for applications that do not want TCP's sequencing or flow control and wish to offer their own.
- It is also used for client-server type request-reply queries and applications in which prompt delivery is more important than accurate delivery such as transmitting speech or video.

### **4) Application Layer:**

- In TCP/IP model, session or presentation layer are not present.
  - Application layer is present on the top of the Transport layer.
  - **It includes all the higher-level protocols which are virtual terminal (TELNET), file transfer (FTP) and electronic mail (SMTP).**
- The virtual terminal protocol permits a user on one machine to log into a distant machine and work there.
  - The file transfer protocol offers a way to move data efficiently from one machine to another.
  - Electronic mail was used for file transfer purpose but later a specialized protocol was developed for it.

#### **The Application Layer defines following protocols:**

##### **i) File Transfer Protocol (FTP):**

- It was designed to **permit reliable transfer of files over different platforms.**

- At the transport layer to ensure reliability, FTP uses TCP.
- FTP offers simple commands and makes the differences in storage methods across networks transparent to the user.
- The FTP client is able to interact with any FTP server; therefore the FTP server must also be able to interact with any FTP client.
- FTP does not offer a user interface, but it does offer an application program interface for file transfer.
- The client part of the protocol is called as FTP and the server part of the protocol is known as FTPd.
- The **suffix "d" means Daemon** this is a legacy from Unix computing **where a daemon is a piece of software running on a server** that offers a service.

### **ii) Hyper Text Transfer Protocol:**

- **HTTP permits applications such as browsers to upload and download web pages.**
- It makes use of TCP at the transport layer again to check reliability.
- HTTP is a **connectionless protocol** that sends a request, receives a response and then disconnects the connection.
- HTTP delivers HTML documents plus all of the other components supported within HTML such as JavaScript, Visual script and applets.

### **iii) Simple Mail Transfer Protocol:**

- **By using TCP, SMTP sends email to other computers that support the TCP/IP protocol suite.**
- SMTP provides extension to the local mail services that existed in the early years of LANs.
- It supervises the email sending from the local mail host to a remote mail host.
- It is not reliable for accepting mail from local users or distributing received mail to recipients this is the responsibility of the local mail system.
- SMTP makes use of TCP to establish a connection to the remote mail host, the mail is sent, any waiting mail is requested and then the connection is disconnected.
- It can also return a forwarding address if the intended recipient no longer receives email at that destination.
- To enable mail to be delivered across differing systems, a mail gateway is used.

**iv) Simple Network Management Protocol**

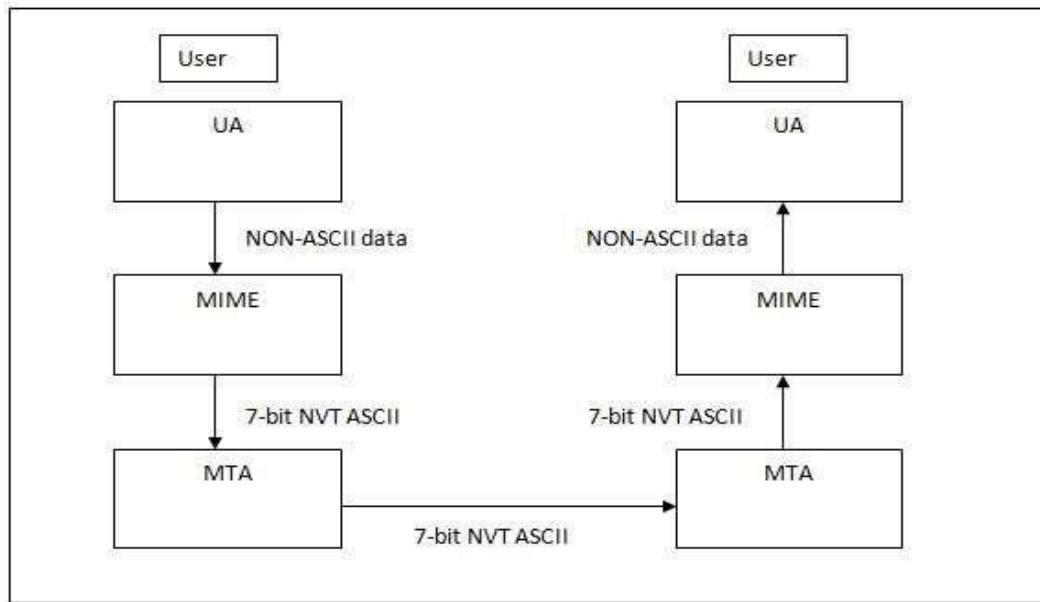
- For the transport of network management information, SNMP is used as standardized protocol.
- Managed network devices can be cross examined by a computer running to return details about their status and level of activity.
- Observing software can also trigger alarms if certain performance criteria drop below acceptable restrictions.
- At the transport layer SNMP protocol uses UDP.
- The use of UDP results in decreasing network traffic overheads.

**6. Explain in details about the MIME protocol with suitable diagram.****Synopsis:****1.6. MIME****Definition****MIME headers**

- 1. MIME-Version**
- 2. Content-Type**
- 3. Content-Transfer-Encoding**
- 4. Content-Id**
- 5. Content-Description**

**1.6. MIME:****Definition:**

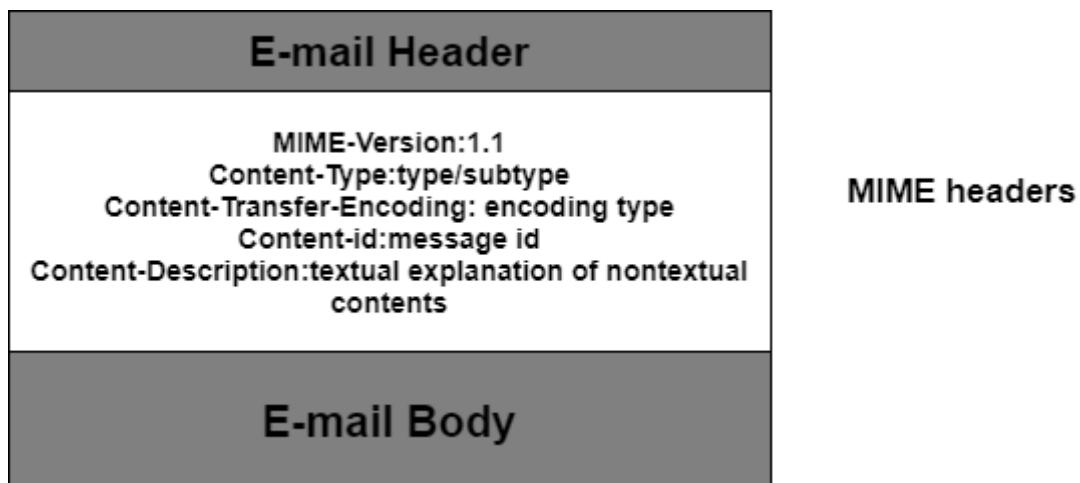
- Multipurpose Internet Mail Extensions (MIME) is a supplementary protocol that allows non-ASCII data to be sent through e-mail.
- MIME transforms non-ASCII data at the sender site to NVT ASCII data and delivers them to the client MTA to be sent through the Internet.
- The message at the receiving side is transformed back to the original data. We can think of MIME as a set of software functions that transforms non-ASCII data (stream of bits) to ASCII data and vice versa, as shown in Figure 1.17.

**Figure 1.17 MIME**

MIME defines five headers that can be added to the original e-mail header Section to define the transformation parameters:

1. MIME-Version
2. Content-Type
3. Content-Transfer-Encoding
4. Content-Id
5. Content-Description

Figure 1.18 shows the MIME headers. We will describe each header in detail

**Figure 1.18 MIME header**

**MIME-Version** This header defines the version of MIME used.

The current version is 1.1.

# MIME-Version: 1.1

MIME allows seven different types of data. These are listed in Table 1.1

**Table 1.1 Data types and subtypes in MIME**

Type	Subtype	Description
Text	Plain	Unformatted
	HTML	HTML format (see Chapter 27)
Multipart	Mixed	Body contains ordered parts of different data types
	Parallel	Same as above, but no order
	Digest	Similar to mixed subtypes, but the default is message/RFC822
	Alternative	Parts are different versions of the same message
Message	RFC822	Body is an encapsulated message
	Partial	Body is a fragment of a bigger message
	External-Body	Body is a reference to another message
Image	IPEG	Image is in IPEG format
	GIF	Image is in GIF format
Video	MPEG	Video is in MPEG format
Audio	Basic	Single-channel encoding of voice at 8 kHz
Application	PostScript	Adobe PostScript
	Octet-stream	General binary data (8-bit bytes)

**7. Explain in details about the SMTP protocol with suitable diagram.**

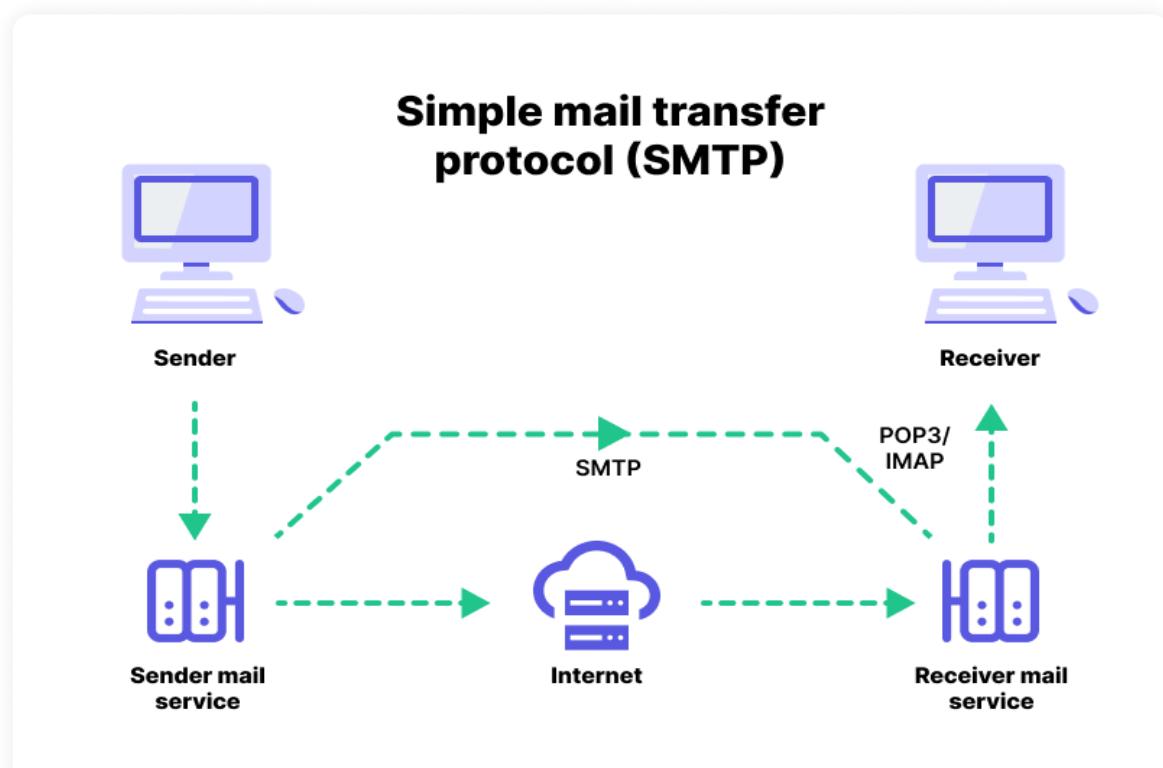
**Synopsis:**

- **Message Transfer Agent: SMTP**
- **Commands and Responses**

**Message Transfer Agent: SMTP**

- The actual mail transfer is done through message transfer agents. To send mail, a system must have the client MTA, and to receive mail, a system must have a server MTA.

- The formal protocol that defines the MTA client and server in the Internet is called the Simple Mail Transfer Protocol (SMTP)
- Figure 1.19 shows the range of the SMTP protocol in this scenario.

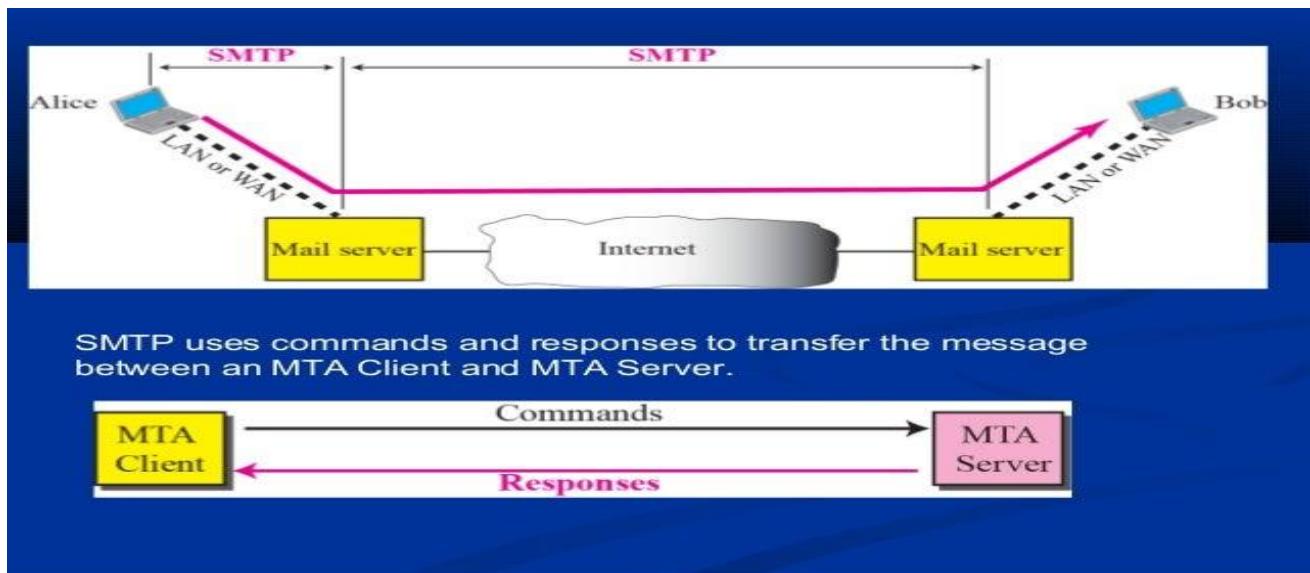


**Figure 1.19 SMTP**

- SMTP is used two times, between the sender and the sender's mail server and between the two mail servers.

#### **Commands and Responses**

- SMTP uses commands and responses to transfer messages between an MTA client and an MTA server (see Figure 1.20).

**Figure 1.20 Commands and responses****8. Explain in details about the POP and IMAP protocol with suitable diagram.****Synopsis:**

- ✓ **Post Office Protocol, version 3 (POP3)**
- ✓ **POP3 has two modes:**
  - Delete mode and
  - Keep mode.
- ✓ **IMAP4**

**Post Office Protocol, version 3 (POP3)**

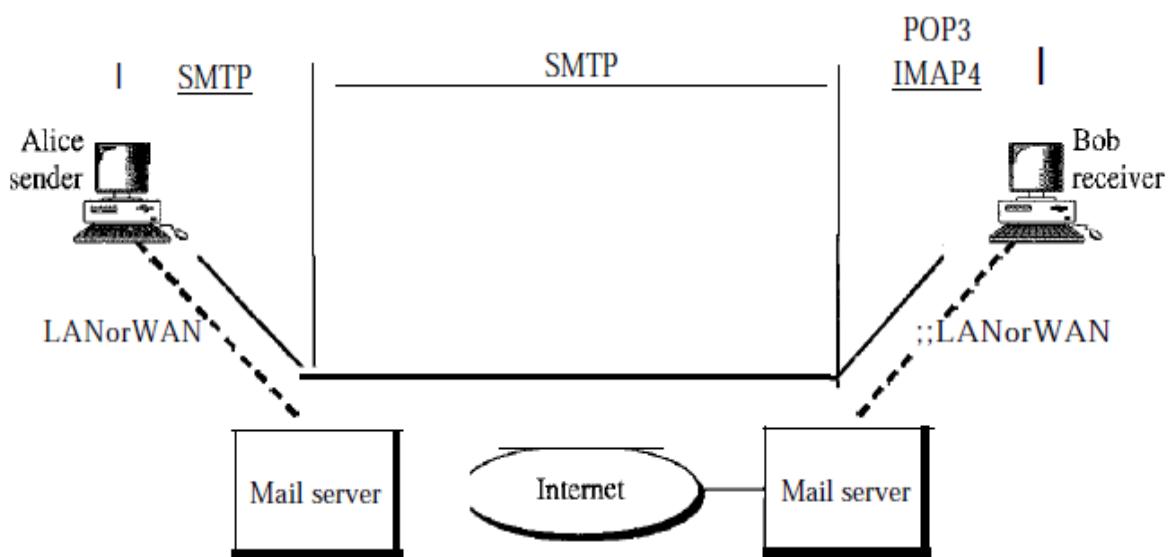
- **Post Office Protocol, version 3 (POP3)** is simple and limited in functionality.
- The client POP3 software is installed on the recipient computer; the server POP3 software is installed on the mail server.
- Mail access starts with the client when the user needs to download e-mail from the mailbox on the mail server.
- The client opens a connection to the server on TCP port 110.
- It then sends its user name and password to access the mailbox. The user can then list and retrieve the mail messages, one by one. Figure 26.20 shows an example of downloading using POP3.

**POP3 has two modes:**

- Delete mode and
- Keep mode.

1. **In the delete mode**, the mail is deleted from the mailbox after each retrieval.

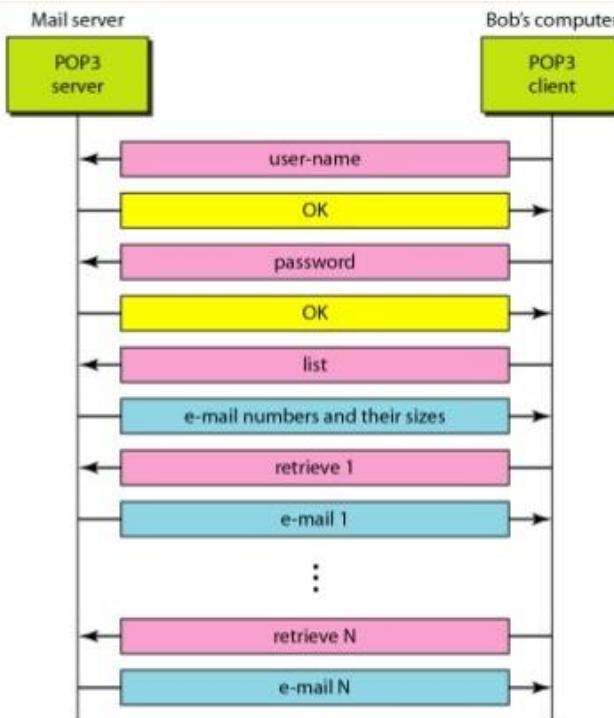
2. **In the keep mode**, the mail remains in the mailbox after retrieval.
3. The **delete mode** is normally used when the user is working at her permanent computer and can save and organize the received mail after reading or replying.
4. The **keep mode** is normally used when the user accesses her mail away from her primary computer (e.g., a laptop). The mail is read but kept in the system for later retrieval and organizing. Figure 1.21 shows the position of these two protocols in the most common situation



**Figure 1.21 POP3 and IMAP4**

#### **IMAP4**

- Another mail access protocol is **Internet Mail Access Protocol, version 4** (IMAP4).
- IMAP4 is similar to POP3, but it has more features; IMAP4 is more powerful and more Complex. Figure 1.22 shows an example of downloading using POP3.



**Figure 1.22 the exchange of commands and responses in POP3**

#### **IMAP4 provides the following extra functions:**

- A user can check the e-mail header prior to downloading.
- A user can search the contents of the e-mail for a specific string of characters prior to downloading.
- A user can partially download e-mail. This is especially useful if bandwidth is limited and the e-mail contains multimedia with high bandwidth requirements.
- A user can create, delete, or rename mailboxes on the mail server.
- A user can create a hierarchy of mailboxes in a folder for e-mail storage.

#### **9.Explain in details about the FTP protocol with suitable diagram.(April/may 2023)**

##### **Synopsis:**

- **File Transfer Protocol (FTP)**
- **Communication over Control Connection**
- **Communication over Data Connection**

##### **File Transfer Protocol (FTP)**

- File Transfer Protocol (FTP) is the standard mechanism provided by TCP/IP for copying a file from one host to another.

- Although transferring files from one system to another seems simple and straightforward, some problems must be dealt with first.
- For example, two systems may use different file name conventions.
- Two systems may have different ways to represent text and data.
- Two systems may have different directory structures. All these problems have been solved by FTP in a very simple and elegant approach.

**FTP uses two well-known TCP ports:**

- Port 21 is used for the control connection,
- port 20 is used for the data connection.

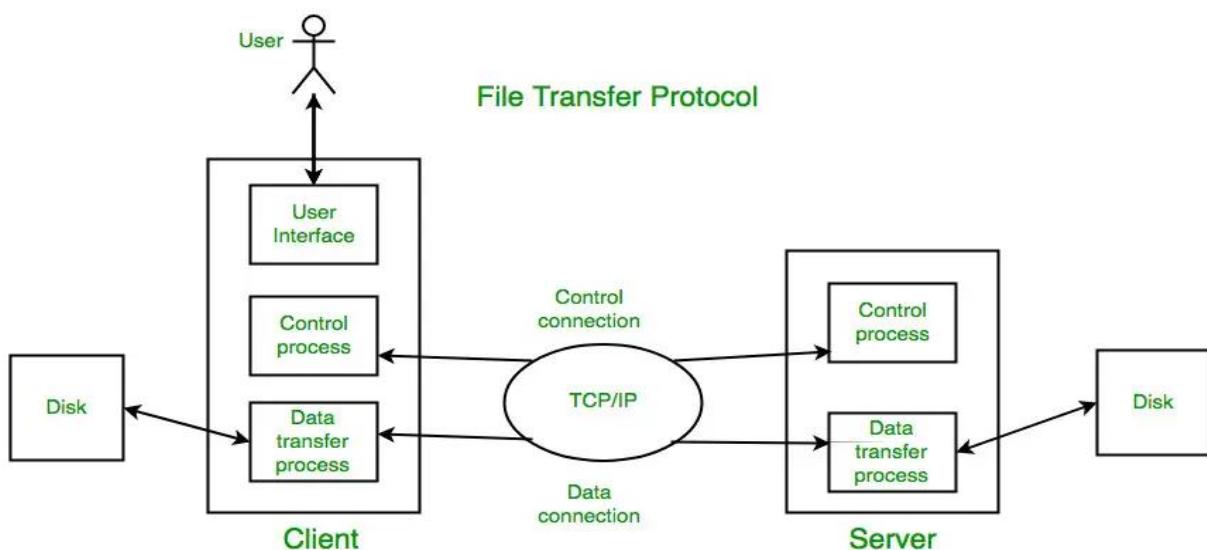
Figure 1.9 shows the basic model of FTP.

**The client has three components:**

- User interface,
- client control process,
- the client data transfer process.

**The server has two components:**

- The server control process
- The server data transfer process.
- The control connection is made between the control processes.
- The data connection is made between the data transfer processes.



**Figure 1.23 FTP**

### **Communication over Control Connection**

- FTP uses the same approach as SMTP to communicate across the control connection.
- It uses the 7-bit ASCII character set (see Figure 1.9 a). Communication is achieved through commands and responses.
- This simple method is adequate for the control connection because we send one command (or response) at a time. Each command or response is only one short line, so we need not worry about file format or file structure.
- Each line is terminated with a two-character (carriage return and line feed) end-of-line token.

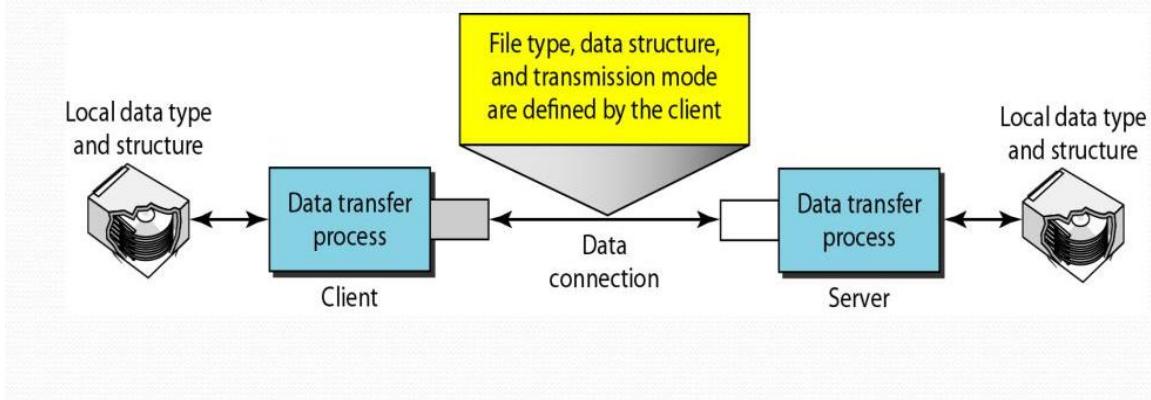


**Figure 1.23 Using the control connection**

### **Communication over Data Connection**

- The purpose of the data connection is different from that of the control connection.
- We want to transfer files through the data connection. File transfer occurs over the data connection under the control of the commands sent over the control connection.
- However, we should remember that **file transfer in FTP means one of three things:**
  - A file is to be copied from the server to the client. This is called retrieving aft/e.
  - It is done under the supervision of the RETR command,
  - A file is to be copied from the client to the server. This is called storing aft/e.
  - It is done under the supervision of the STOR command.(see fig.1.24).
  - A list of directory or file names is to be sent from the server to the client.
  - This is done under the supervision of the LIST command. **Note that FTP treats a list of directory or file names as a file. It is sent over the data connection.**

## Using the data connection



**Figure 1.24 using the data connection**

### 10. Explain in detail about topology and its types.

**Synopsis:**

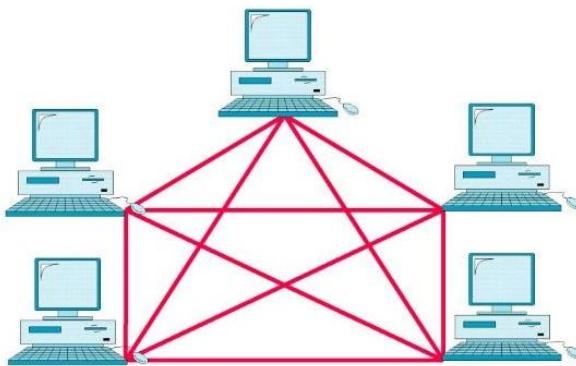
- **Network Topologies**
  1. Mesh Topology
  2. Star Topology
  3. Tree Topology
  4. Bus Topology
  5. Ring Topology
  6. Hybrid Topology

#### **Network Topologies**

- Topology refers to the way a network is laid out either physically or logically.
- Two or more devices connect to a link; two or more links form a topology.
- It is the geographical representation of the relationship of all the links and linking devices to each other.
  1. Mesh
  2. Star
  3. Tree
  4. Bus
  5. Ring
  6. Hybrid

### 1. Mesh Topology:

- **Here every device has a dedicated point to point link to every other device.**
- A fully connected mesh can have  $n(n-1)/2$  physical channels to link  $n$  devices. It must have  $n-1$  IO ports. (Refer fig 1.25)



**Fig 1.25 – Mesh**

#### **Advantages:**

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

#### **Disadvantages:**

1. The amount of cabling and the number IO ports required are very large. Since every device is connected to each other devices through dedicated links.
2. The sheer bulk of wiring is larger then the available space
3. Hardware required to connect each device is highly expensive.

#### **Example:**

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

#### **Solution:**

$$\text{Number of devices} = 8$$

$$\text{Number of links} = n(n-1)/2$$

$$= 8(8-1)/2$$

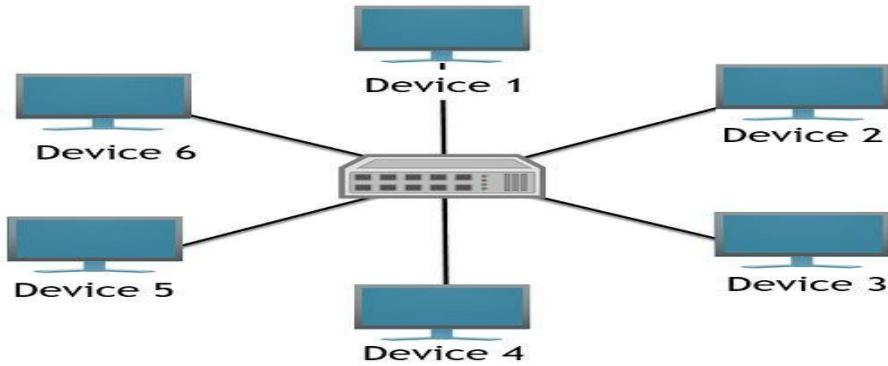
$$= 28$$

$$\text{Number of port/device} = n-1$$

$$= 8-1 = 7$$

## 2. STAR TOPOLOGY:

- Here each device has a **dedicated link to the central ‘hub’.**
- There is no direct traffic between devices. The transmission are occurred only through the central controller namely hub. (Refer fig 1.26)



**Fig 1.26 – Star**

### Advantages:

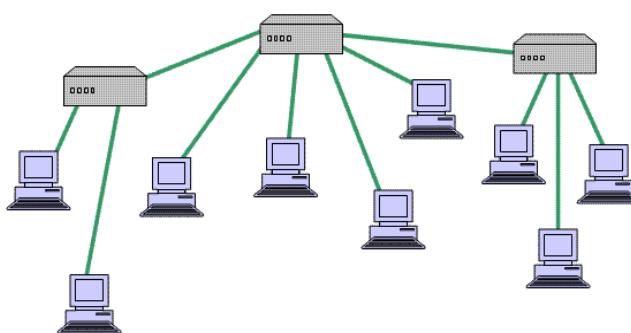
1. Less expensive than mesh since each device is connected only to the hub.
2. Installation and configuration are easy.
3. Less cabling is needed than mesh.
4. Robustness.
5. Easy to fault identification & isolation.

### Disadvantages:

1. Even if it requires less cabling than mesh when compared with other topologies, it is still large.

## 3. TREE TOPOLOGY:

- It is a variation of star. Instead of all devices connected to a central hub here most of the **devices are connected to a secondary hub that in turn connected with central hub.**
- The central hub is an active hub. An active hub contains a repeater, which regenerates the received bit pattern before sending. (Refer fig 1.27)



**Fig 1.27 – Tree**

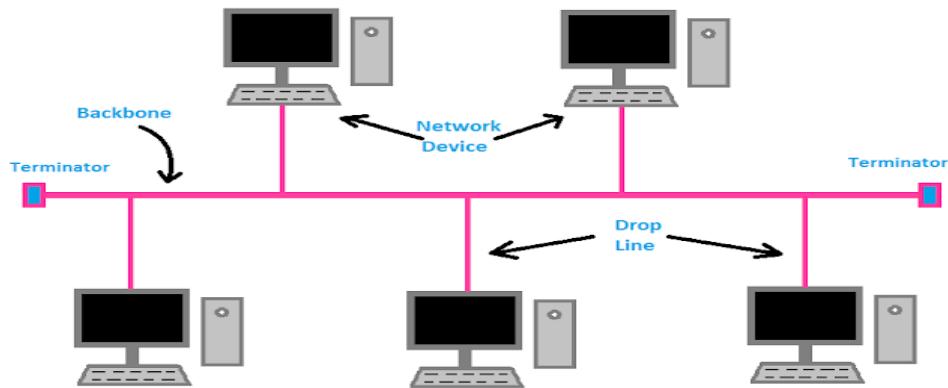
- The secondary hub may be active or passive. A passive hub means it just precedes a physical connection only.

**Advantages:**

- Can connect more than star.
- The distance can be increased.
- Can isolate and prioritize communication between different computers.

**4. BUS TOPOLOGY:**

- A bus topology is multipoint.
- Here one long cable is act as a backbone to link all the devices are connected to the backbone by drop lines and taps.
- A drop line is the connection between the devices and the cable.
- A tap is the splice into the main cable or puncture the sheathing. (Refer fig 1.28)



**Fig 1.28 – Bus**

**Advantages:**

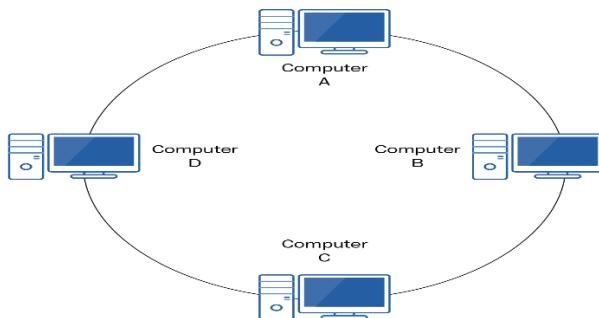
- Ease of installation.
- Less cabling.

**Disadvantages:**

- Difficult reconfiguration and fault isolation.
- Difficult to add new devices.
- Signal reflection at top can degradation in quality
- If any fault in backbone can stops all transmission

### 5. Ring topology

- **Each node is connected to exactly two other nodes, forming a ring.** Can be visualized as a circular configuration.
- Requires at least three nodes (Refer fig 1.29)



**Fig 1.29 – Ring**

#### Advantages:

1. Easy to install.
2. Easy to reconfigure.
3. Fault identification is easy.

#### Disadvantages:

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

### 6. Hybrid topology

- A combination of any two or more network topologies.

### 11. Discuss briefly DNS (Domain Name System)& its advantages 2017 (or)

**Demonstrate how request of a Domain name fetches its IP**

**Address from DNS server and establish connection with the server.**

**(Nov 2021). (April/may 2024)**

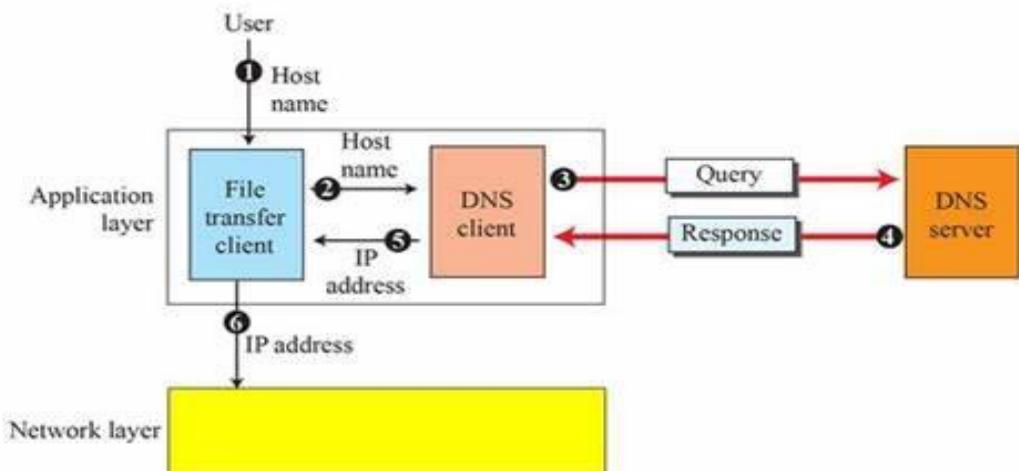
#### Synopsis:

- **DNS (Domain Name System) – Definition.**
- **Namespace**
- **Flat Namespace**
- **Hierarchical Namespace**
- **Domain Hierarchy**
- **Domain Name**
- **Types of Domain Name**
- **Fully Qualified Domain Name (FQDN)**

- **Partially Qualified Domain Name (PQDN)**
- **Three main components of DNS**
  1. **Resolver**
  2. **Name server**
  3. **Database of Resource Records (RRs)**
- **Name Servers**
- **Name Server Types**
- **DNS Messages**
- **DDNS**
  - ✓ **Advantages**

**Definition:**

- **The DNS translates Internet domain and host names to IP addresses.**
- DNS automatically converts the names we type in our Web browser address bar to the IP addresses of Web servers hosting those sites.



**Fig 1.30 – Purpose of DNS**

The following six steps map the host name to an IP address: (Refer fig 1.30)

1. The user passes the host name to the file transfer client.
2. The file transfer client passes the host name to the DNS client.
3. Each computer, after being booted, knows the address of one DNS server. The DNS client sends a message to a DNS server with a query that gives the file transfer server name using the known IP address of the DNS server.
4. The DNS server responds with the IP address of the desired file transfer server.
5. The DNS server passes the IP address to the file transfer client.

6. The file transfer client now uses the received IP address to access the file transfer server.

#### **Namespace:**

- **The names assigned to computers must be selected from a name space.**
- **The name must be unique because the addresses are unique.**
- A namespace that maps each address to a unique name can organize in two ways.
  1. Flat Namespace
  2. Hierarchical Namespace

##### **i. Flat Namespace:**

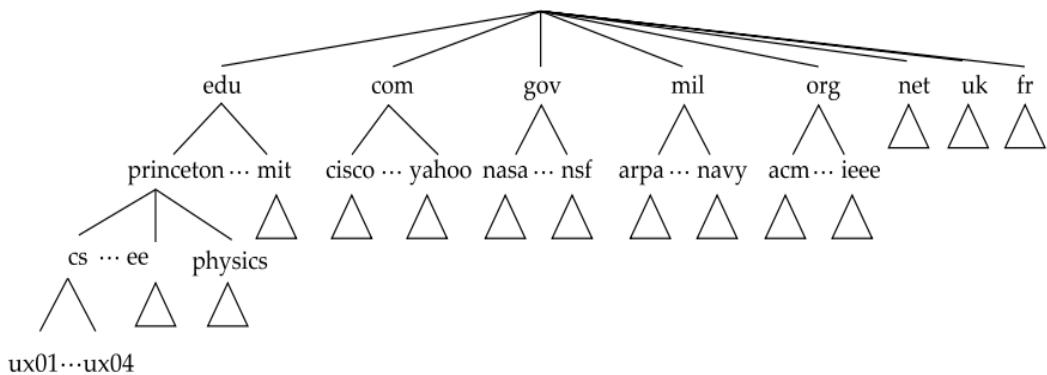
- **A name is assigned to an address.**
- **A name in this space is a sequence of characters without structure.**
- The main disadvantage of flat namespace is that, it cannot use in a large system such as the internet.

##### **ii. Hierarchical Namespace:**

- **Each name is made of several parts.**
- **The first part can define the nature of the organization, the second part can define the name, and the third part can define department and so on.**
- The authority to assign and control the namespaces can be decentralized.

#### **Domain Hierarchy:**

- **DNS is hierarchical in structure. A domain is a subtree of the domain name space.**
- **All the related information about a particular network (generally maintained by an organization, firm or university) should be available at one place.**
- The organization should have complete control over what it includes in its network and how does it "organize" its network. Meanwhile, all this information should be available transparently to the outside world.
- **Conceptually, the internet is divided into several hundred top level domains where each domain covers many hosts. Each domain is partitioned in subdomains which may be further partitioned into sub subdomains and so on... So the domain space is partitioned in a tree like structure** as shown below (Refer fig 1.31).
- The internet uses a hierarchical tree structure of Domain Name Servers for IP address resolution of a host name.

**Fig 1.31 – Domain Hierarchy**

- The top level domains are either generic or names of countries. eg of generic top-level domains are .edu .mil .gov .org .net .com .int etc. For countries we have one entry for each country as defined in ISO3166. eg. .in (India) .uk (United Kingdom).
- The leaf nodes of this tree are target machines.
- Obviously we would have to ensure that the names in a row in a subdomain are unique.
- The max length of any name between two dots can be 63 characters. The absolute address should not be more than 255 characters.
- Domain names are case insensitive.
- Also in a name only letters, digits and hyphen are allowed. For eg. **www.iitk.ac.in** is a domain name corresponding to a machine named www under the sub domain iitk.ac.in.

### **Domain Name**

- A name that identifies one or more **IP addresses**.
- For example, the domain name *microsoft.com* represents about a dozen IP addresses.
- Domain names are used in **URLs** to identify particular **Web pages**. For example, in the URL *http://www.pcwebopedia.com/index.html*, the domain name is *pcwebopedia.com*.

### **Types of Domain Name**

1. Fully Qualified Domain Name (FQDN)
2. Partially Qualified Domain Name (PQDN)

**1. FQDN:**

- A fully qualified domain name (FQDN) consists of the host name plus domain name. e.g. **computername.domain.com**

**2. PQDN:**

- A partially Qualified Domain Name (PQDN) starts from a node, but it does not reach the root. e.g. **computer name**

**Three main components of DNS**

1. Resolver
2. Name server
3. Database of Resource Records (RRs)

**➤ Resolver:**

- **A host that needs to map an address to a name or a name to an address calls a DNS client called a resolver.**
- The resolver accesses the closest DNS server with a mapping request.
- If the server has the information, it satisfies the resolver; after the resolver receives the mapping, it interprets the response to see if it's a real resolution or an error, and finally delivers the result to the process that requested it.

**i) Mapping names to address**

- The resolver gives a domain name to the server and asks for the corresponding address.

**ii) Mapping address to names**

- A client can send an IP address to a server to be mapped to a domain name.

**iii) Recursive resolution**

- The resolver can ask for a recursive answer from a name server.
- This means that the resolver expects the server to supply the final answer. If the server is the authority for the domain name, it checks its database and responds. When the query is finally resolved, the response travels back until it finally reaches the requesting client. This is called recursive resolution.

**iv) Iterative resolution**

- If the client doesn't ask for a recursive answer, the mapping can be done iteratively.
- If the newly addressed server can resolve the problem, it answers the query with the IP address.
- Otherwise it returns the IP address of a new server to a client. Now the

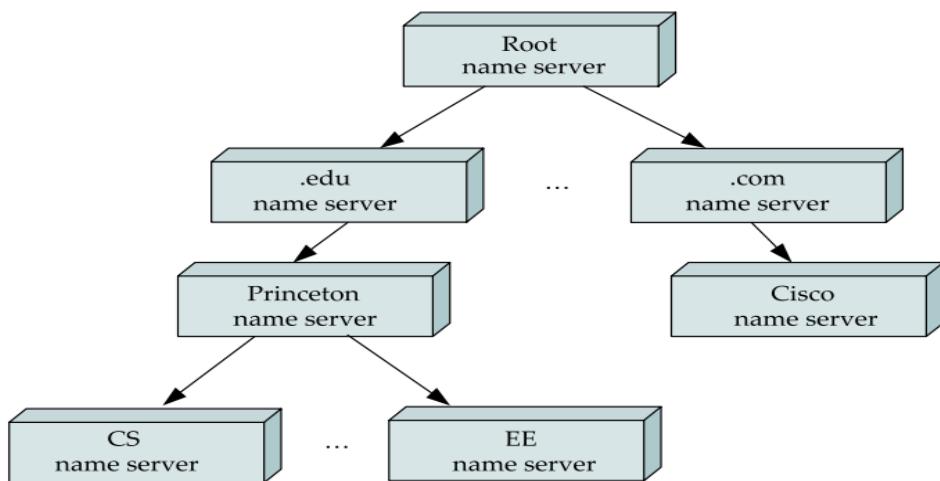
client must repeat the query to the second server. **This process is called iterative resolution** because the client repeats the same query to multiple servers.

#### v) Caching

- Each time a server receives a query for a name that is not in its domain, it needs to search its database for a server IP address.
- Reduction of this time put increase efficiency. When a server asks for a mapping from another server and receives the response, it stores this information in its cache memory before sending it to the client. If the same or another client asks for the same mapping, it can check its cache memory and solve the problem. This mechanism is called caching.

#### Name Servers

- **The first step is to partition the hierarchy into sub trees called zones.**
- Each zone can be thought of a corresponding to some administrative authority that is responsible for that portion of the hierarchy.
- **DNS server is used to distribute the information among many computers.**
- Specifically, the information contained in each zone is implemented in two or more name servers for the sake of redundancy, that is, the information is still available even if one name server fails. Each name server, in turn, is a program that can be accessed over the Internet.
- Client send queries to name servers, and name servers respond with the requested information. Sometimes the response contains the final answer that the client wants, and sometimes the response contains a pointer to another server that the client should query next.

**Fig 1.32 – Name server**

### **Name Server Types**

Name server types are: (Refer fig 1.32)

#### **1. Root Server :**

- A root server is a server whose zone consist of the whole tree. A root server usually does not store any information about domains. But delegates its authority to other servers, keeping references to those servers.

#### **2. Primary Server:**

- A Primary server is a server that stores a file about the zone for which it is an authority. It is responsible for creating, maintaining and updating the zone file. It stores the zone file on a local disk.

#### **3. Secondary Server:**

- A secondary server transfers the complete information about a zone from another server and stores the file on its local disk.
- The secondary server neither creates nor updates the zone files. If updating is required it must be done by the primary server, which sends the updated version to the secondary. When the secondary downloads information from the primary it is called zone transfer.

### **Types of Records**

There are two types of records are used in DNS.

1. The question records
2. Resource Records

**1. The question records:** Is used by the client to get information from a server. This contains a domain name.

#### **2. Resource Records:**

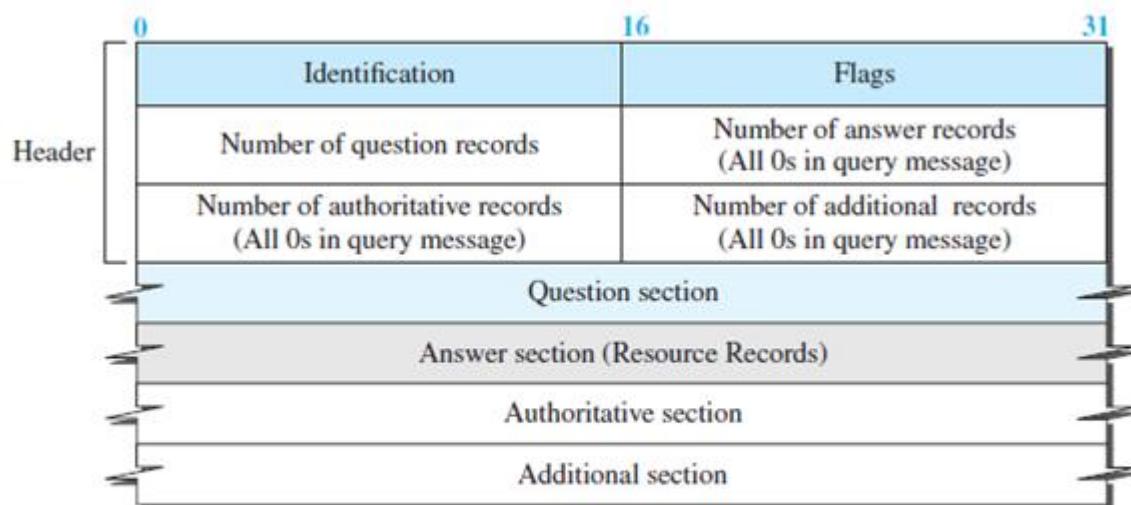
- Each domain name is associated with a record called the resource record. The server database consists of resource records. The resource records are used in the answer, authoritative and additional information section of the response message.
- Each name server implements the zone information as a collection of resource records. In essence, a resource record is a name-to-value binding, **a 5-tuple that contains the following fields: (Refer table 1.2)**
  - **Domain name:** the domain to which this record applies.
  - **Class:** set to IN for internet information. For other information other codes may be specified.
  - **Type:** tells what kind of record it is.
  - **Time to live:** Upper Limit on the time to reach the destination
  - **Value:** can be an IP address, a string or a number depending on the record type.

<b>Resource Record Type</b>	<b>Contents</b>	<b>Use</b>
A	Host Address	Used to hold a specific host's IP address.
CNAME	Canonical Name (alias)	Used to make an alias name for a host.
MX	Mail Exchanger	Provides message routing to a mail server, plus backup server(s) in case the target server isn't active.
NS	Name Server	Provides a list of authoritative servers for a domain or indicates authoritative DNS servers for any delegated sub-domains.
PTR	Pointer	Used for reverse lookup—resolving an IP address into a domain name using the IN-ADDR.ARPA domain.

SOA	Start of Authority	Used to determine the DNS server that's the primary server for a DNS zone and to store other zone property information.
-----	--------------------	---

**Table 1.2- Resource records****DNS Messages**

- To retrieve information about hosts, DNS uses two types of messages: *query* and *response*. Both types have the same format (Refer fig 1.33)

**Note:**

The query message contains only the question section.  
The response message includes the question section, the answer section, and possibly two other sections.

**Fig 1.33 – DNS message****DDNS**

- When the DNS was designed, no one predicted that there would be so many address changes.
- In DNS, when there is a change, such as adding a new host, removing a host, or changing an IP address, the change must be made to the DNS master file. These types of changes involve a lot of manual updating. The size of today's Internet does not allow for this kind of manual operation. The DNS master file must be updated dynamically.
- The **Dynamic Domain Name System (DDNS)** therefore was devised to respond to this need.
- In DDNS, when a binding between a name and an address is determined, the information is sent, usually by DHCP to a primary DNS server To provide security

and prevent unauthorized changes in the DNS records, DDNS can use an authentication mechanism.

#### **Advantages:**

**More Reliable:** Delivers messages to the users with zero downtime.

**Faster:** DNS are connected well at intersections of internet. Anycast technology enables requests are answered to the next closest node in the case of maintenance or downtime.

**Smarter:** Automatic corrections of typos.

### **12. Briefly Explain the concept of SNMP (Simple Network Management**

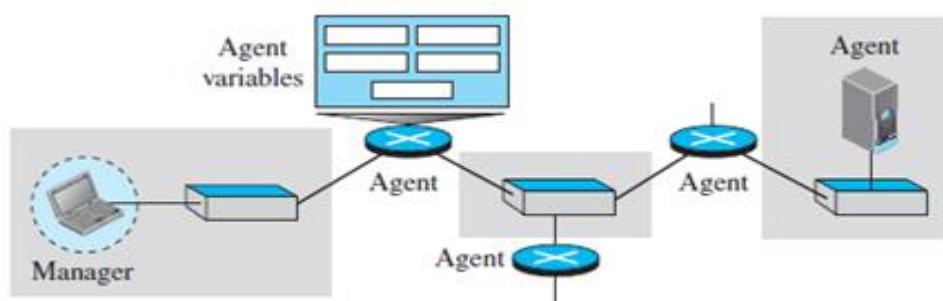
**Protocol) (Apr /may2011) (May 2015) (Nov 2016) (April/may 2023)**

#### **Definition:**

SNMP is a frame work for managing devices in an internet using TCP/IP suite. It provides fundamental operations for monitoring and maintaining an internet.

#### **Concept:**

- SNMP uses the concept of manager and agent.
- Manager usually a host controls and monitors a set of agents, usually routers.
- A management station, called a manager, is a host that runs the SNMP client program.
- A managed station, called an agent, is a router or host that runs the SNMP server program.
- Management is achieved through simple interaction between a manager and an agent.
- The agent keeps performance information in a database. The manager has access to the values in the database. (Refer fig 1.34)



**Fig 1.34 – SNMP concept**

### Managers and Agents

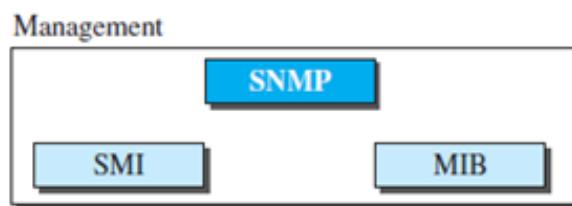
- A management station, called a *manager*, is a host that runs the SNMP client program.
- A managed station, called an *agent*, is a router (or a host) that runs the SNMP server program.
- Management is achieved through simple interaction between a manager and an agent.
- The agent keeps performance information in a database.
- The manager has access to the values in the database.

### Management with SNMP is based on three basic ideas

1. A manager checks an agent by requesting information that reflects the behavior of the agent.
2. A manager forces an agent to perform a task by resetting values in the agent database.
3. An agent contributes the management process by warning the manager of an unusual situation.

### Management Components

- To do management tasks, SNMP uses two other protocols: **Structure of Management Information (SMI)** and **Management Information Base (MIB)**.
- In other words, management on the Internet is done through the cooperation of three protocols: SNMP, SMI, and MIB (Refer fig 1.35).



**Fig 1.35 – Components of network management on the Internet**

### Role of SNMP

- SNMP has some very specific roles in network management.
- **It defines the format of the packet to be send from a manager to an agent and vice versa.**
- It also interprets the result and creates statistics.
- The packet exchange contains the object names (variables) and their status (values).

- SNMP is response for reading and changing these values.

#### **Role of SMI**

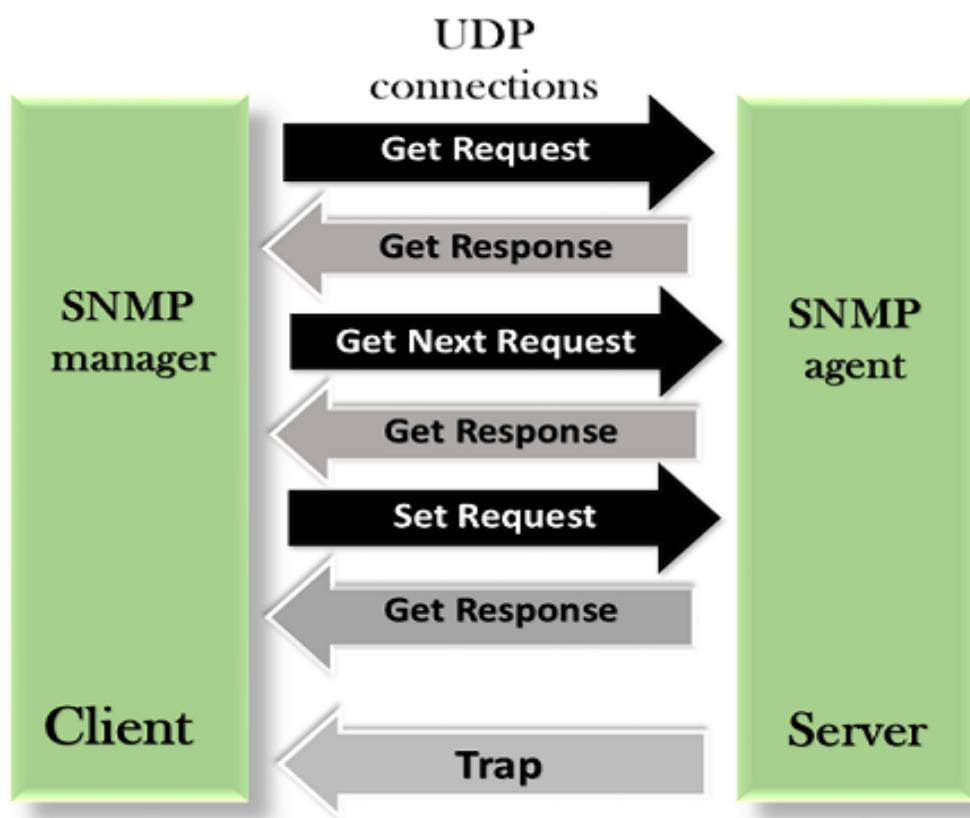
- SMI defines the general rules for naming objects, defining object types (including range and length), and showing how to encode objects and values.

#### **Role of MIB**

- MIB creates a collection of named objects, their types, and their relationships to each other in an entity to be managed

#### **PDU's**

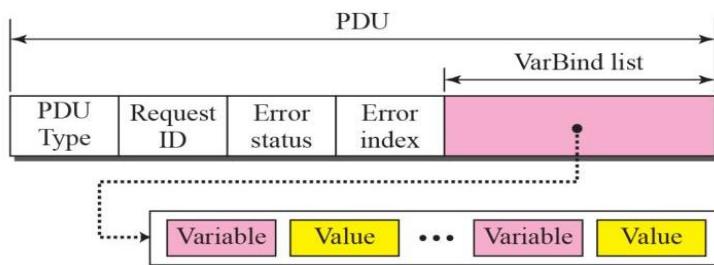
- SNMP V3 defines 8 types of packets (Refer fig 1.36)



**Fig 1.36 – SNMP V3 packets**

<b>PDU Type</b>	<b>Name</b>	<b>Description</b>
1	get-request	Get one or more variables .(manager to agent)
2	get-next-request	Get next variable after one or more specified variables. (manager to agent)
3	Get-bulk-request	To retrieve a large amount of data

4	set-request	Set one or more variables. (manager to agent)
5	get-response	Return value of one or More variables. (agent to manager)
6	trap	Notify manager of an event. (agent to manager)
7	Inform request	To get the value of some variable from agents under the control of the remote manager. The remote manager response with a response PDU. ( one manager to another remote manager)
8	report	To report some types of errors between managers.

**Table 1.3– PDU type****SNMP PDU Format**

Differences:

1. Error status and error index values are zeros for all request messages except GetBulkRequest.
2. Error status field is replaced by non-repeater field and error index field is replaced by max-repetitions field in GetBulkRequest.

**Fig 1.37 – SNMP PDU format**

- **PDU type** - This field defines the type of the PDU.
- **Request ID** – This field is a sequence number used by the manager in a request PDU and repeated by the agent in a response. It is used to match a request to a response.
- **Error status** – This is an integer that is used only in response PDU's to show the types of errors reported by the agent. Its value is zero in request PDU's. (Refer fig 1.37)

**Types of errors:**

Error	Name	Description
0	no error	OK
1	too big	Reply does not fit into one message
2	no such name	The variable specified does not exist
3	bad value	Invalid value specified in a set request.
4	read only	The variable to be changed is read only.
5	general error	General error

**Table 1.4 – Errors**

**Non Repeater:** This field is used only in get-bulk-request and replaces the error status field which is empty in request PDU's.

- **Error Index:** Error index is an offset that tells the manager which variable caused the error.

**Max-repetition:** This field is also used only in get-bulk-request and replaces the error index filed, which is empty in request PDU's

- **Var Bind List:** This is a set of variables with corresponding values the manager wants to retrieve or set. The values or null in get-request and get-next-request.

**SNMP messages:**

- SNMP does not send only a PDU, it embeds the PDU in a message. A message in SNMPv3 is made of four elements: version, header, security parameter and data.
- The **version**, defines the current version (3).
- The **header** contains values for message identification, maximum message size, message flag and a message security model.
- The message **security parameter** is used to create a message digest.
- The **data** contain the PDU. If the data are encrypted, there is information about the encrypting engine and the encrypting context followed by the encrypted PDU. If the data are not encrypted, the data consist of just the PDU.

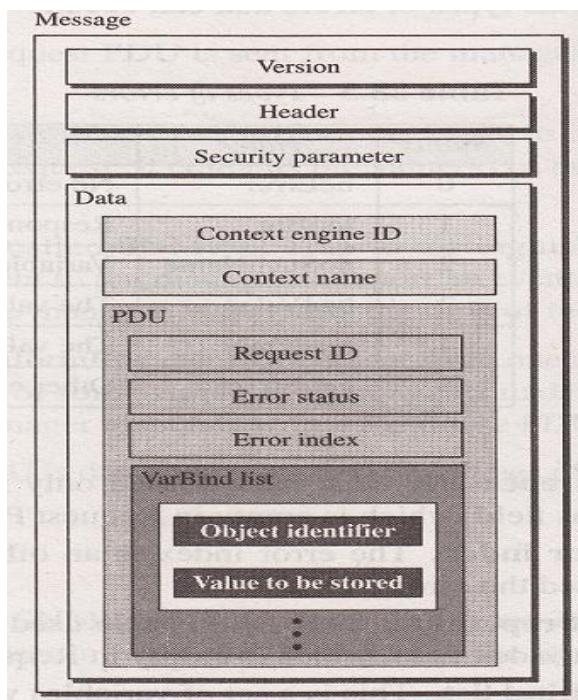
**UDP Ports:**

- SNMP uses the services of UDP **on two well-known ports, 161 and 162.**

- The well-known **port 161 is used by the server (agent)**, and the well-known **port 162 is used by the client (Manager)**. (Refer fig 1.38)

**Security:**

- SNMPv3 provides two types of security: general and specific.
- SNMPv3 provides message authentication, privacy, and manager authorization.
- SNMPv3 allows a manager remotely change the security configuration, which means that the manager does not have to be physically present at the manager station.



**Fig 1.38 – SNMP UDP ports**

**13) What is HTTP protocol used for? (OR) Write notes on URLs(NOV/DEC**

**2014) (Nov 2015) (May 2016) (Nov/Dec 2020)**

**ii) What is the default port number of HTTP protocol?**

**iii) Discuss the features of HTTP and also discuss how HTTP works.**

**HTTP PROTOCOL**

- The **HyperText Transfer Protocol (HTTP)** is used to define how the client-server programs can be written to retrieve web pages from the Web.
- An HTTP client sends a request; an HTTP server returns a response.
- The server uses the port number 80; the client uses a temporary port number.
- Protocol for transfer of data between Web servers and Web clients (browsers).

- “The Hypertext Transfer Protocol (HTTP) is an **application-level protocol** for **distributed**, collaborative, hypermedia information systems.
- Popular Web servers:
  - Apache HTTPD, JBoss and Tomcat
- Popular Web clients:
  - Firefox and Opera

### **HTTP Properties**

#### **1) A comprehensive addressing scheme**

- The HTTP protocol uses the concept of reference provided by the **Universal Resource Identifier (URI) as a location (URL) or name (URN)**, for indicating the resource on which a method is to be applied.
- Every resource accessible through HTTP is identified by a Uniform Resource Location (URL), which is a location-specific identifier.
  - For example,
    - <http://www.cs.uct.ac.za:80/>
    - <ftp://ftp.cs.uct.ac.za/>
- A Uniform Resource Identifier (URI) is a standard format (<scheme>:<identifier>) generic identifier.
  - For example,
    - mailto:hussein@cs.uct.ac.za
- A Uniform Resource Name (URN) is one example of a location-independent URI.
  - For example urn:isbn:123-456-789

#### **2) Client-Server architecture**

- **The HTTP protocol is based on a request/response paradigm.**
- The communication generally takes place over a TCP/IP connection on the Internet.
- **The default port is 80**, but other ports can be used.
- A requesting program (a client) establishes a connection with a receiving program (a server) and sends a request to the server in the form of a request method, URI, and protocol version, followed by a message containing request modifiers, client information, and possible body content.
- The server responds with a status line, including its protocol version and a success or error code, followed by a message containing server information, entity meta-information, and possible body content.

***3) HTTP protocol is connectionless***

- This HTTP protocol is called connectionless because once the single request has been satisfied, the connection is dropped.

***4) HTTP protocol is stateless***

- After the server has responded to the client's request, the connection between client and server is dropped and forgotten.
- There is no "memory" between client connections.
- The pure HTTP server implementation treats every request as if it was brand-new (without context), i.e. not maintaining any connection information between transactions.

**Other HTTP Features**

- Persistent connections
- Cache control

**Persistent Connections**

- Persistent connections provide a mechanism by which a client and a server can signal the close of a TCP connection.
- With them, it is possible to establish a TCP connection, send a request and get a response, and then send additional requests and get additional responses.
- By amortizing the TCP setup and release over multiple requests, the relative overhead due to TCP is much less per request.
- It is also possible to pipeline requests, that is, send request 2 before the response to request 1 has arrived.

**Persistent HTTP connections have a number of advantages:**

- By opening and closing fewer TCP connections, CPU time is saved in routers and hosts (clients, servers, proxies, gateways, tunnels, or caches), and memory used for TCP protocol control blocks can be saved in hosts.
- HTTP requests and responses can be pipelined in a connection.
- Pipelining allows a client to make multiple requests without waiting for each response, allowing a single TCP connection to be used much more efficiently, with much lower elapsed time.

**Caching**

- The goal of caching in HTTP is to eliminate the need to send requests in many cases, and to eliminate the need to send full responses in many other cases.
- That is, there are two main reasons that web caching is used:

- 1) To reduce latency because the request is satisfied from the cache (which is closer to the client) instead of the origin server, it takes less time for the client to get the object and display it. This makes Web sites seem more responsive.
- 2) To reduce traffic because each object is only gotten from the server once, it reduces the amount of bandwidth used by a client. This saves money if the client is paying by traffic, and keeps their bandwidth requirements lower and more manageable.

### **Nonpersistent versus Persistent Connections**

➤ **Nonpersistent Connections**

In a **nonpersistent connection**, one TCP connection is made for each request/response.

The following lists the steps in this strategy:

1. The client opens a TCP connection and sends a request.
2. The server sends the response and closes the connection.
3. The client reads the data until it encounters an end-of-file marker; it then closes the connection.

➤ **Persistent Connections**

HTTP version 1.1 specifies a **persistent connection** by default. In a persistent connection, the server leaves the connection open for more requests after sending a response. The server can close the connection at the request of a client or if a time-out has been reached. The sender usually sends the length of the data with each response.

### **Message Formats**

The HTTP protocol defines the format of the request and response messages

### **Request Message**

### **HTTP Methods**

HTTP allows an open-ended set of methods to be used to indicate the purpose of a request. The three most often used methods are **GET**, **HEAD**, and **POST**. (Refer table 1.5)

<b>Method</b>	<b>Description</b>
OPTIONS	capabilities of resource/server
GET	retrieve resource
HEAD	retrieve headers for resource
POST	submit data to server

PUT	replace/insert resource on server
DELETE	remove resource from server
TRACE	trace request route through Web

**Table 1.5 – HTTP Methods*****The GET method***

The GET method requests the server to send the page. The page is suitably encoded in MIME. The vast majority of requests to Web servers are GETs. The usual form of GET is GET filename HTTP/1.1 Where filename names the resource (file) to be fetched and 1.1 is the protocol version being used.

***The Head Method***

The HEAD method is used to ask only for information about a document, not for the document itself. HEAD is much faster than GET, as a much smaller amount of data is transferred. It's often used by clients who use caching, to see if the document has changed since it was last accessed. If it was not, then the local copy can be reused, otherwise the updated version must be retrieved with a GET.

***The PUT method***

The PUT method is the reverse of GET: instead of reading the page, it writes the page. This method makes it possible to build a collection of Web pages on a remote server.

***The POST method***

The POST method is used to transfer data from the client to the server.

***DELETE***

DELETE does what you might expect: it removes the page. There is no guarantee that DELETE succeeds, since even if the remote HTTP server is willing to delete the page

***TRACE***

The TRACE method is for debugging. It instructs the server to send back the request. This method is useful when requests are not being processed correctly and the client wants to know what request the server actually got.

***OPTION***

The OPTIONS method provides a way for the client to query the server about its properties or those of a specific file. Telling whether the request was satisfied, and if not, why not.

Status	Reason	Description
200	OK	Successful request
206	Partial Content	Successful request for partial content
301	Moved Permanently	Resource has been relocated
304	Not Modified	Conditional GET but resource has not changed
400	Bad Request	Request not understood
403	Forbidden	Access to resource not allowed
404	Not Found	URI/resource not found on server
500	Internal Server Error	Unexpected error

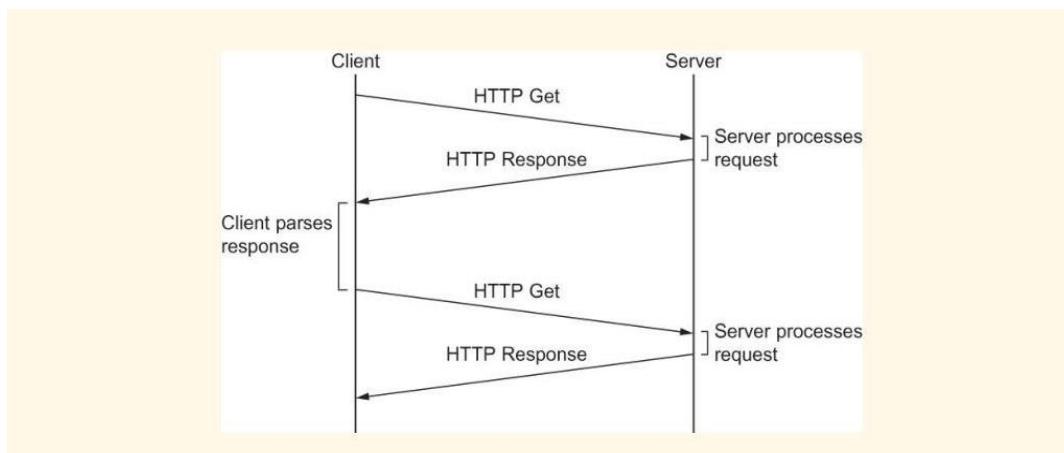
**Table 1.6 – HTTP status****HTTP Header Fields(Nov/Dec 2007)**

Header	Description
User-agent	Identifies the client program
Accept	Shows the media format the client can accept
Accept-charset	Shows the character set the client can handle
Accept-encoding	Shows the encoding scheme the client can handle
Accept-language	Shows the language the client can accept
Authorization	Shows what permissions the client has
Host	Shows the host and port number of the client
Date	Shows the current date
Upgrade	Specifies the preferred communication protocol
Cookie	Returns the cookie to the server (explained later)
If-Modified-Since	If the file is modified since a specific date

**Table 1.7 – Request header names**

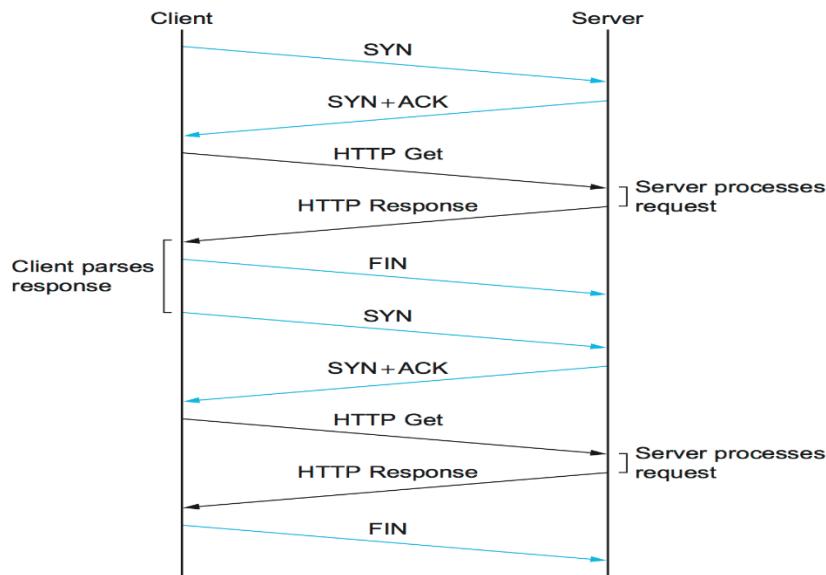
- An HTTP transaction consists of a header followed optionally by an empty line and some data.
- The header will specify such things as the action required of the server, or the type of data being returned, or a status code.
- The use of header fields sent in HTTP transactions gives the protocol great flexibility.
- These fields allow descriptive information to be sent in the transaction, enabling authentication, encryption, and/or user identification.

- The header is a block of data preceding the actual data, and is often referred to as meta information, because it is information about information. (Refer fig 1.24)
- **Accept:** Indicates which data formats are acceptable.
  - Accept: text/html, text/plain
- **HTTP\_User-Agent.**
  - The browser the client is using to send the request.
  - **General format:** software/version library/version.
- **Content-Language:** Language of the content
  - Content-Language: English
- **Content-Length:** Size of message body
  - Content-Length: 1234
- **Content-Type:** MIME type of content body
  - Content-Type: text/html



**Fig 1.36 – HTTP 1.1 behavior with persistent connections**

- **Date:** The Date header represents the date and time at which the message was originated
  - Date: Tue, 15 Nov 1994 08:12:31 GMT
- **Expires:** When content is no longer valid
  - Expires: Tue, 15 Nov 1994 08:12:31 GMT
- **Host:** Machine that request is directed to
  - Host: www.cs.uct.ac.za

**Fig 1.37 – HTTP 1.0 behavior**

➤ **Location:**

The Location response header field defines the exact location of the resource that was identified by the request URI. If the value is a full URL, the server returns a "redirect" to the client to retrieve the specified object directly.

- Location: <http://myserver.org/>

➤ **Retry-After:** Indicates that client must try again in future

- Retry-After: 120

**Response Message**

- A response message consists of a status line, header lines, a blank line, and sometimes a body.
- The first line in a response message is called the *status line*.
- There are three fields in this line separated by spaces and terminated by a carriage return and line feed (Refer table 1.8)

<i>Header</i>	<i>Description</i>
Date	Shows the current date
Upgrade	Specifies the preferred communication protocol
Server	Gives information about the server
Set-Cookie	The server asks the client to save a cookie
Content-Encoding	Specifies the encoding scheme
Content-Language	Specifies the language
Content-Length	Shows the length of the document
Content-Type	Specifies the media type
Location	To ask the client to send the request to another site
Accept-Ranges	The server will accept the requested byte-ranges
Last-modified	Gives the date and time of the last change

**Table 1.8 – Response header names**



(Approved by AICTE, New Delhi, Affiliated to Anna University Chennai, Accredited by NBA, TCS & NAAC - 'A' Grade)

## DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND DATA SCIENCE

II YEAR / IV SEM

### CS3591 – COMPUTER NETWORKS

#### **UNIT II TRANSPORT LAYER**

Introduction - Transport-Layer Protocols: UDP – TCP: Connection Management – Flow control - Congestion Control - Congestion avoidance (DECbit, RED) – SCTP – Quality of Service.

#### **PART-A**

##### **1. List the duties of Transport Layer (TL)**

- Packetizing
- Connection Control
- Addressing
- Providing reliability

##### **2. What is the difference between TCP & UDP? (NOV 2014 & 2016)**

<b>TCP</b>	<b>UDP</b>
• Connection Oriented Service	• Connection less Service
• Reliable	• Not much reliable
• Not suitable for multimedia, real time applications	• used for multimedia and multicast applications

##### **3. What is socket? Define socket address.**

- **Socket is the end point of a bi-directional communication flow across IP based network (Internet).**
- Socket address is the combination of an IP address (location of computer) and a port (application program process) into a single entity.

#### 4. What is congestion? How to control congestion? (Nov/Dec 2020)

- Congestion in network is the situation in which an increase in data transmission results in a **reduction in the throughput**.
- Throughput-amount of data passes through network congestion can be controlled using two techniques.
  - Open-loop congestion control (prevention)
  - Closed-loop congestion control(removal)

#### 5. Define jitter

- Jitter is the **variation in delay** for packets belonging to the same flow.

Example: 2ms delay for 1<sup>st</sup> packet

60ms delay for second packet.

#### 6. What is the use of integrated services?

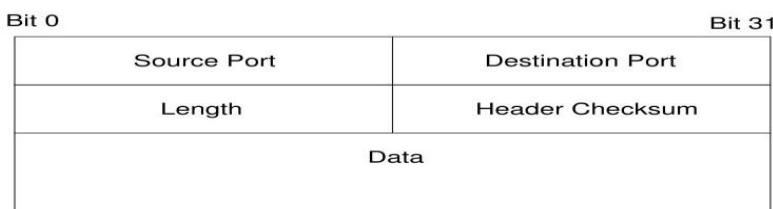
Integrated services (Instserv) is a followed based QoS model where the user creates a flow from source to direction and inform all the routers of the resource requirement.

#### 7. Differentiate between delay and jitter.

- Voice over IP (VoIP) is susceptible to network behaviors, referred to as delay and jitter, which can degrade the voice application to the point of being unacceptable to the average user.
- **Delay is the time taken from point-to-point in a network.** Delay can be measured in either one-way or round-trip delay.
- **Jitter is the VARIATION in delay over time from point-to-point.** If the delay of transmissions varies too widely in a VoIP call, the call quality is greatly degraded. The amount of jitter tolerable on the network is affected by the depth of the jitter buffer on the network equipment in the voice path. The more jitter buffer available, the more the network can reduce the effects of jitter.

#### 8. Draw UDP header format.

### UDP Header Format



**9. What is traffic shaping?**

Traffic shaping is a mechanism to **control the amount and rate of traffic** sent to the network.

**10. What is the unit of data transfer in UDP and TCP?**

In UDP, the Unit of data transfer is called datagram.

In TCP, Unit of data transfer is called segments.

**11. List the timers used by TCP.**

- 1) Retransmission timer
- 2) Persistence timer
- 3) Keep alive timer
- 4) Time waited timer

**12. Define Sill window syndrome.**

Sending less amount of Data (Ex. 1 byte) which is lesser than header size (20 bytes of TCP header +20 bytes of IP header) is called **silly window syndrome**.

Here the capacity of network is used inefficiently.

**13. Explain the main idea of UDP Or Simple Demultiplexer.**

The basic idea is for a source process to send a message to a port and for the destination process to receive the message from a port.

**14. What are the different fields in pseudo header?**

- Protocol number
- Source IP address
- Destination IP addresses.

**15. Define TCP Or Reliable byte stream.**

TCP guarantees **the reliable, in order delivery of a stream of bytes**.

It is a full-duplex protocol, meaning that each TCP connection supports a pair of byte streams, one flowing in each direction.

**16. Define Congestion Control.**

It involves **preventing too much data from being injected into the network**, thereby causing switches or links to become overloaded. Thus flow control is an end to an end issue, while congestion control is concerned with how hosts and networks interact.

**17. State the two kinds of events trigger a state transition.**

- A segment arrives from the peer.
- The local application process invokes an operation on TCP.

**18. What is meant by segment?**

At the sending and receiving end of the transmission, **TCP divides long transmissions into smaller data units and packages each into a frame called a segment.**

**19. What is meant by segmentation?**

When the size of the data unit received from the upper layer is too long for the network layer datagram or data link layer frame to handle, **the transport protocol divides it into smaller usable blocks. The dividing process is called segmentation.**

**20. What is meant by Concatenation?**

- The size of the data unit belonging to single sessions are so small that several can fit together into a single datagram or frame, the transport protocol combines them into a single data unit.
- The combining process is called concatenation.

**21. What is rate based design?**

Rate- based design, in which the receiver tells **the sender the rate-expressed in either bytes or packets per second** – at which it is willing to accept incoming data.

**22. Define Gateway.**

A device used to connect two separate networks that use different communication protocols.

**23. What are the two categories of QoS attributes?**

The two main categories are,

- User Oriented
- Network Oriented

**24. What is RED?**

**Random Early Detection** in each router is programmed to monitor its own queue length and when it detects that congestion is imminent, to notify the source to adjust its congestion window.

**25. What are the three events involved in the connection?**

For security, the transport layer may create a connection between the two end ports. A connection is a single logical path between the source and destination that is associated with all packets in a message. Creating a connection involves three steps:

- Connection establishment
- Data transfer
- Connection release

**26. Give the approaches to improve the QoS.**

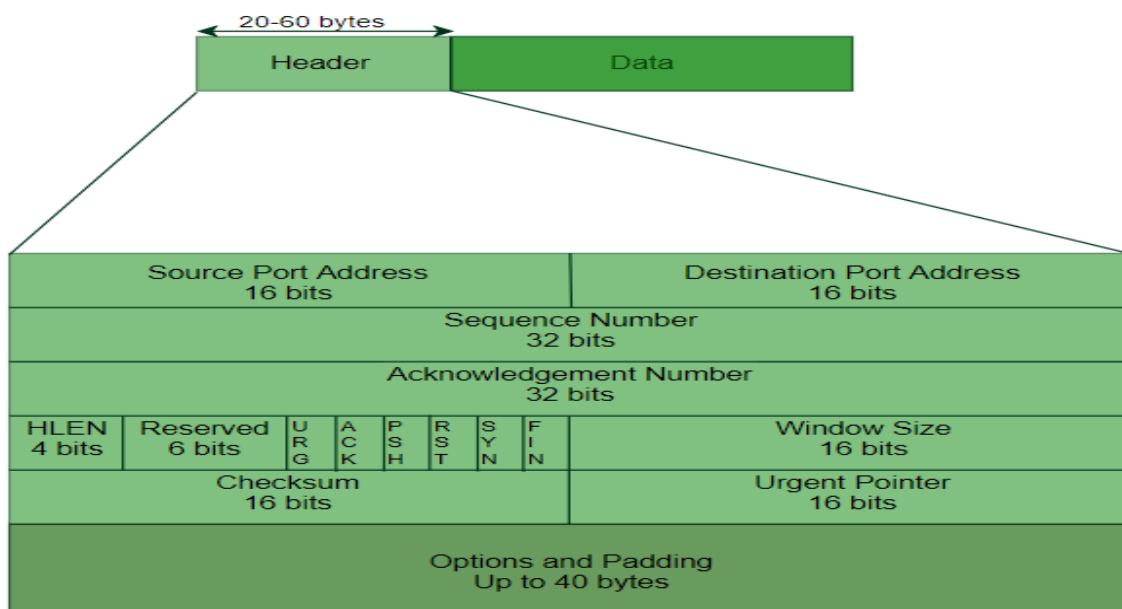
Four common techniques are:

- Scheduling
- Traffic shaping
- Admission control
- Resource reservation

**27. What is the difference between service point address, logical address and physical address? Service point addressing Logical addressing Physical addressing.**

Service point addressing	Logical addressing	Physical addressing
The transport layer header includes a type of address called a service point address or port address, which makes a data delivery from a specific process on one computer to a specific process on another computer.	If a packet passes the network boundary we need another addressing to differentiate the source and destination systems. The network layer adds a header, which indicates the logical address of the sender and receiver.	If the frames are to be distributed to different systems on the network, the data link layer adds a header, which defines the source machine's address and the destination machine's address.

**28. Draw TCP header format.**



**29. How will the congestion be avoided?**

The congestion may be avoided by two bits

**BECN** - Backward Explicit Congestion Notification

**FECN** - Forward Explicit Congestion Notification

**30. What is the function of BECN BIT?**

The BECN bit warns the sender of congestion in network. The sender can respond to this warning by simply reducing the data rate.

**31. What is the function of FECN?**

- The FECN bit is used to warn the receiver of congestion in the network.
- The sender and receiver are communicating with each other and are using some types of flow control at a higher level.

**32. What is meant by quality of service or QoS? (NOV 2014 & 2015)**

- **The quality of service defines a set of attributes related to the performance of the connection.**
- For each connection, the user can request a particular attribute each service class is associated with a set of attributes.

**33. List out the user related attributes.**

User related attributes are

**SCR** – Sustainable Cell Rate

**PCR** – Peak Cell Rate

**MCR** - Minimum Cell Rate

**CVDT** – Cell Variation Delay Tolerance

**34. What are the networks related attributes?**

The network related attributes are,

Cell loss ratio (CLR)

Cell transfer delay (CTD)

Cell delay variation (CDV)

Cell error ratio (CER)

**35. Why is UDP pseudo header included in UDP checksum calculation?**

**What is the effect of an invalid checksum at the receiving UDP?**

- The UDP checksum is performed over the entire payload, *and* the other fields in the header, *and* some fields from the IP header.

- A pseudo-header is constructed from the IP header in order to perform the calculation (which is done over this pseudo-header, the UDP header and the payload).
- **The reason the pseudo-header is included is to catch packets that have been routed to the wrong IP address.**
- If the checksum validation is enabled and it detected an invalid checksum, features like packet reassembling won't be processed.

**36. How can the effect of jitter be compensated? What type of application require for this compensation?**

- Jitter is an undesirable effect caused by the inherent tendencies of TCP/IP networks and components.
- Jitter is defined as a variation in the delay of received packets.
- The sending side transmits \ packets in a continuous stream and spaces them evenly apart.
- Because of network congestion, improper queuing, or configuration errors, the delay between packets can vary instead of remaining constant.
- This variation causes problems for audio playback at the receiving end.
- Playback may experience gaps while waiting for the arrival of variable delayed packets.
- When a router receives an audio stream for VoIP, it must compensate for any jitter that it detects.
- The playout delay buffer mechanism handles this function.
- Playout delay is the amount of time that elapses between the time a voice packet is received at the jitter buffer on the DSP and the time a voice packet is played out to the codec.
- The playout delay buffer must buffer these packets and then play them out in a steady Stream to the DSPs.
- The DSPs then convert the packets back into an analog audio stream.
- The play out delay buffer is also referred to as the dejitter buffer.

**37. What is meant by PORT or MAILBOX related with UDP?**

- Form of address used to identify the target process:
  - ✓ **Process can directly identify each other with an OS-assigned process ID(pid) More commonly- processes indirectly identify each other using a port or mailbox Source sends a message to a port and destination receives the message from the port UDP port is 16**

**bits**, so, there are 64K possible ports- not enough for all Internet hosts  
Process is identified as a port on a particular host – a (port, host) pair.

- ✓ To send a message the process learns the port in the following way:
- ✓ A client initiates a message exchange with a server process.
- ✓ The server knows the client's port (contained in message header and can reply to it. Server accepts messages at a well-known port.

**Examples: DNS at port 53, mail at port 25**

### **38. List out the various features of sliding window protocol.**

- The key feature of the sliding window protocol is that it permits **pipelined communication**.
- In contrast, with a simple stop-and-wait protocol, the sender waits for An acknowledgment after transmitting every frame.
- Throughput, the amount of data in transit at any given time As a result, there is at most a single outstanding frame on the channel at any given time, which may be far less than the channel's capacity. For maximum should be equal to (channel bandwidth) X (channel delay).

### **39. What is the function of a router?**

- Connect network segment together
- Router forwards the packet to the right path.

### **40. What is the advantage of using UDP over TCP?**

- UDP can send data in a **faster** way than TCP
- UDP is suitable for sending **multicasting and multimedia applications**.

### **41. What is the difference between congestion control and flow control?**

**Nov 2015, Nov/Dec 2017.**

#### **Congestion control**

- It involves preventing too much data from being injected into the network, thereby causing switches or links to become overloaded.
- Thus flow control is an end-to-end issue, while congestion control is concerned with how hosts and networks interact.

#### **Flow control**

- The amount of data flowed from source to destination should be restricted.
- The source can send one byte at a time, but it will take long time to transmit n bytes

**42. List the mechanisms used in TCP congestion control mechanism.**

- Additive Increase/Multiplicative Decrease
- Slow Start
- Fast Retransmit and Fast Recovery

**43. List the mechanisms used in TCP congestion avoidance.**

- DEC bit
- RED(Random Early Detection)
- Source-based Congestion Avoidance

**44. Define DEC bit**

- **Each router monitors the load it is experiencing and explicitly notifies the end nodes when congestion is about to occur.**
- This notification is implemented by setting a binary congestion bit in the packets that flow through the router, hence the name *DEC bit*.

**45. What is meant by Source-Based Congestion Avoidance?**

- The general idea of these techniques is to **watch for some sign from the network that some router's queue is building up and that congestion will happen soon if nothing is done about it.**

**46. List the approaches to QoS support or what are the approaches used to provide range of Quality of services. (Nov/Dec 2017).**

1. **Fine-grained approaches**, which provide QoS to individual applications or flows.
2. **Coarse-grained approaches**, which provide QoS to large classes of data or aggregated traffic.

**47. List the types of application requirements in QoS.**

- Real-time.
- Non-real-time.

**48. List some of the Quality-of-service parameters of transport layer. (May 2015)**

- Reliability
- Delay
- Jitter
- Bandwidth

**49. How does transport layer perform duplication control? (May 2015)**

Duplication can be controlled by the use of **sequence number & acknowledgment number**.

**50. What do you mean by slow start in TCP congestion? (May 2016)**

The sender **starts with a very slow rate of transmission** but increases the rate rapidly to reach a threshold.

**51. List the different phases used in TCP connection.**

- ✓ Connection establishment and Data transfer.
- ✓ Connection termination.

**52. List out the advantages of connection oriented services over connectionless services. (APR 2017)****Advantage of connection oriented:**

- (i) In connection oriented virtual circuit, buffers can be reversed in advance
- (ii) Sequencing can be guaranteed
- (iii) Short-headers can be used
- (iv) Troubles caused by delayed duplicate packets can be avoided

**Advantage of connectionless:**

- (i) It can be used over subnets that do not use virtual circuit inside
- (ii) No circuit setup time required
- (iii) It is higher robust in the face of router failure
- (iv) It is best for connectionless transport protocol because it does not impose unnecessary overhead

**53. How do fast retransmit mechanism of TCP works? (APR 2017)**

The transmission rate will be increases with slow start algorithm until either a loss is detected, or the receiver's advertised window (rwnd) is limiting factor, or when the slow start threshold (ssthresh) is reached.

**54. What is a Port? (Nov 2021)**

- Ports are virtual places within an operating system where network connections start and end. They help computers sort the network traffic they receive.
- A port number is a way to identify a specific process to which an internet or other network message is to be forwarded when it arrives at a server.

**55. Define Stream control Transmission Protocol.(Nov 2021).**

- Stream Control Transmission Protocol (SCTP) is a transport-layer protocol that ensures reliable, in-sequence transport of data.
- SCTP provides multihoming support where one or both endpoints of a connection can consist of more than one IP address.

**56. Define Quality of Service(QoS)?(April/may 2023)**

- **Quality of service (QoS)** is the use of mechanisms or technologies that work on a network to control traffic and ensure the performance of critical applications with limited network capacity.
- It enables organizations to adjust their overall **network traffic** by prioritizing specific high-performance applications.

**57. Write about Humming code?(April/may 2023)**

- Hamming code is an error-correcting code used to ensure data accuracy during transmission or storage.
- Hamming code detects and corrects the errors that can occur when the data is moved or stored from the sender to the receiver.
- This simple and effective method helps improve the reliability of communication systems and digital storage. It adds extra bits to the original data, allowing the system to detect and correct single-bit errors.

**58. List the features of connection oriented services?(April/may 2024)**

- connection-oriented service, packets are transmitted to the receiver in the same order the sender has sent them.
- It uses a handshake method that creates a connection between the user and sender for transmitting the data over the network. Hence it is also known as a reliable network service.

**PART - B****1. Discuss in detail about transport layer & its services.****Synopsis:**

- **Introduction**
- **Transport-Layer Services**
- **Process-to-Process Communication**
- **Addressing: Port Numbers**
- **ICANN Ranges**
- **Socket Addresses**
- **Encapsulation and Encapsulation**
- **Multiplexing and Demultiplexing**
- **Flow Control**
- **Error Control**
- **Congestion Control**
- **Connectionless and Connection-Oriented Protocols**

**INTRODUCTION**

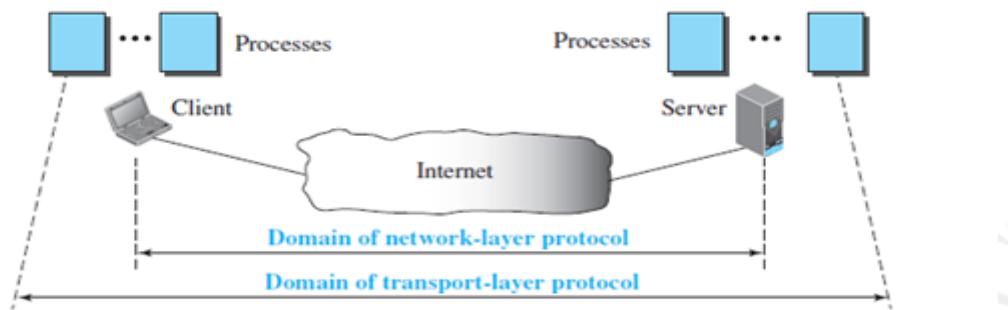
- The transport layer is located between the application layer and the network layer.
- It provides a process-to-process communication between two application layers, one at the local host and the other at the remote host.
- Communication is provided using a logical connection, which means that the two application layers, which can be located in different parts of the globe, assume that there is an imaginary direct connection through which they can send and receive messages.

**Transport-Layer Services**

- **Each protocol provides a different type of service** and should be used appropriately.
1. **UDP:** UDP is an unreliable connectionless transport-layer protocol used for its simplicity and efficiency in applications where error control can be provided by the application-layer process.
  2. **TCP:** TCP is a reliable connection-oriented protocol that can be used in any application where reliability is important.
  3. **SCTP:** SCTP is a new transport-layer protocol that combines the features of UDP and TCP.

### Process-to-Process Communication

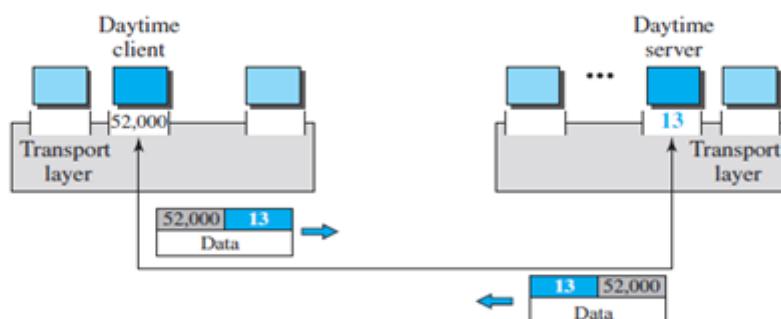
- The first duty of a transport-layer protocol is to provide **process-to-process communication**.
- A process is an application-layer entity (running program) that uses the services of the transport layer.
- A transport-layer protocol is responsible for delivery of the message to the appropriate process (Refer fig 2.1)



**Fig 2.1 – Network layer verses transport layer**

### Addressing: Port Numbers

- Although there are a few ways to achieve process-to-process communication, the most common is through the **client-server paradigm**.
- A process on the local host, called a *client*, needs services from a process usually on the remote host, called a *server*. (Refer fig 2.2).
- The local host and the remote host are defined using IP addresses. To define the processes, we need second identifiers, called **port numbers**.
- 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.
- An ephemeral port number is recommended to be greater than 1023 for some client/server programs to work properly.



**Fig 2.2 – Port numbers**

Port	Protocol	UDP	TCP	SCTP	Description
7	Echo	✓	✓	✓	Echoes back a received datagram
9	Discard	✓	✓	✓	Discards any datagram that is received
11	Users	✓	✓	✓	Active users
13	Daytime	✓	✓	✓	Returns the date and the time
17	Quote	✓	✓	✓	Returns a quote of the day
19	Chargen	✓	✓	✓	Returns a string of characters
20	FTP-data		✓	✓	File Transfer Protocol
21	FTP-21		✓	✓	File Transfer Protocol
23	TELNET		✓	✓	Terminal Network
25	SMTP		✓	✓	Simple Mail Transfer Protocol
53	DNS	✓	✓	✓	Domain Name Service
67	DHCP	✓	✓	✓	Dynamic Host Configuration Protocol
69	TFTP	✓	✓	✓	Trivial File Transfer Protocol
80	HTTP		✓	✓	HyperText Transfer Protocol
111	RPC	✓	✓	✓	Remote Procedure Call
123	NTP	✓	✓	✓	Network Time Protocol
161	SNMP-server	✓			Simple Network Management Protocol
162	SNMP-client	✓			Simple Network Management Protocol

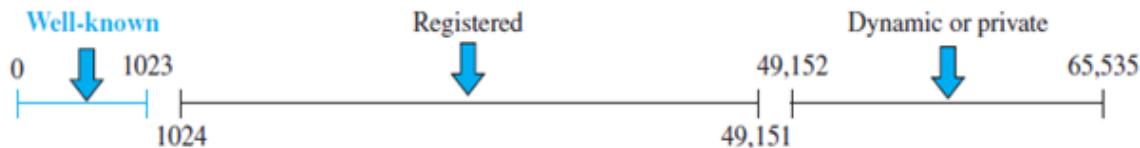
**Table 2.1 – Port numbers****ICANN Ranges**

- ICANN has divided the port numbers into three ranges: well-known, registered, and dynamic (or private), as shown in Figure 2.3.

**Well-known ports.** The ports ranging from 0 to 1023 are assigned and controlled by ICANN. These are the well-known ports.

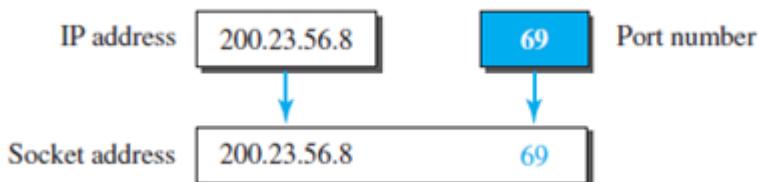
**Registered ports.** The ports ranging from 1024 to 49,151 are not assigned or controlled by ICANN. They can only be registered with ICANN to prevent duplication.

**Dynamic ports.** The ports ranging from 49,152 to 65,535 are neither controlled nor registered. They can be used as temporary or private port numbers.

**Fig 2.3 – ICANN ranges**

### Socket Addresses

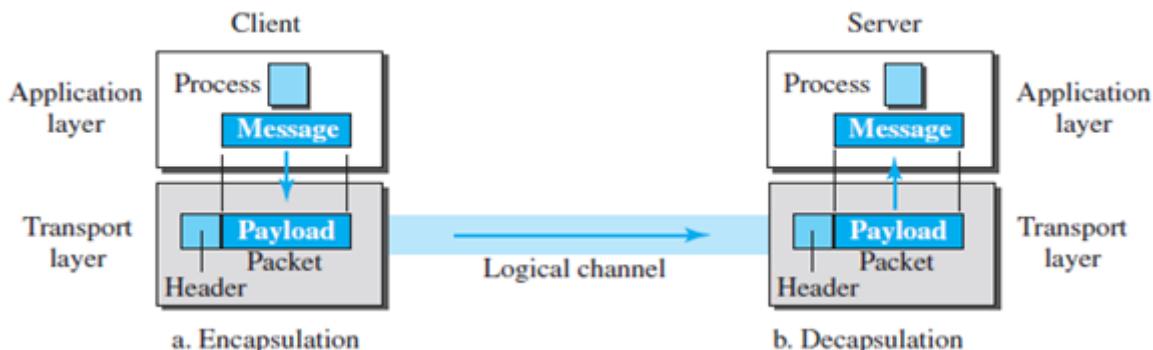
- A transport-layer protocol in the TCP suite needs both the IP address and the port number, at each end, to make a connection.
- The combination of an IP address and a port number is called a **socket address**.
- The client socket address defines the client process uniquely just as the server socket address defines the server process uniquely (Refer fig 2.4).



**Fig 2.4 – Socket address**

### Encapsulation and Encapsulation

- To send a message from one process to another, the transport-layer protocol encapsulates and decapsulates messages. (Refer fig 2.5)



**Fig 2.5 – Encapsulation and Decapsulation**

### Multiplexing and Demultiplexing

- Whenever an entity accepts items from more than one source, this is referred to as **multiplexing** (many to one); whenever an entity delivers items to more than one source, this is referred to as **demultiplexing** (one to many).
- The transport layer at the source performs multiplexing; the transport layer at the destination performs demultiplexing.

### Flow Control

- Whenever an entity produces items and another entity consumes them, there should be a balance between production and consumption rates.

### Error Control

Error control at the transport layer is responsible for,

1. Detecting and discarding corrupted packets.
2. Keeping track of lost and discarded packets and resending them.

3. Recognizing duplicate packets and discarding them.
4. Buffering out-of-order packets until the missing packets arrive.

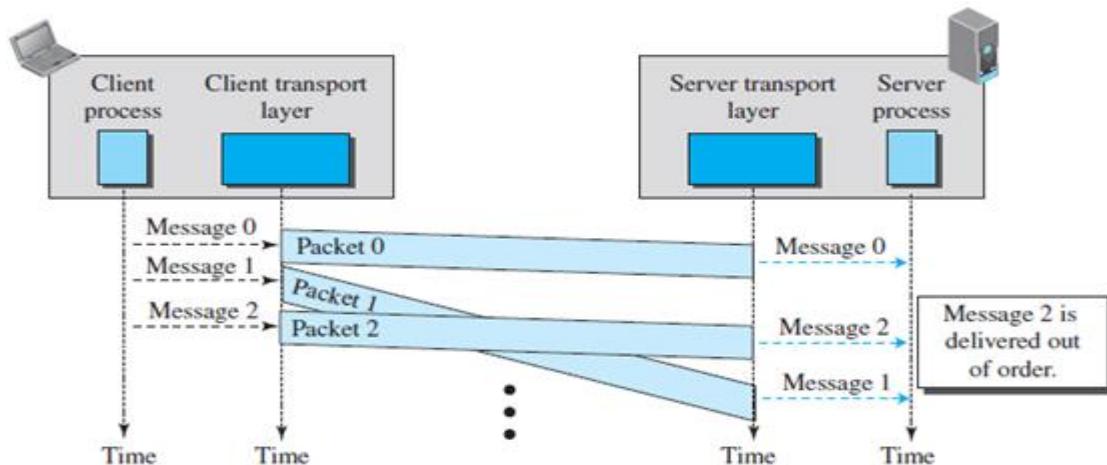
### Congestion Control

- **Congestion control** refers to the mechanisms and techniques that control the congestion and keep the load below the capacity.

### Connectionless and Connection-Oriented Protocols

#### Connectionless Service

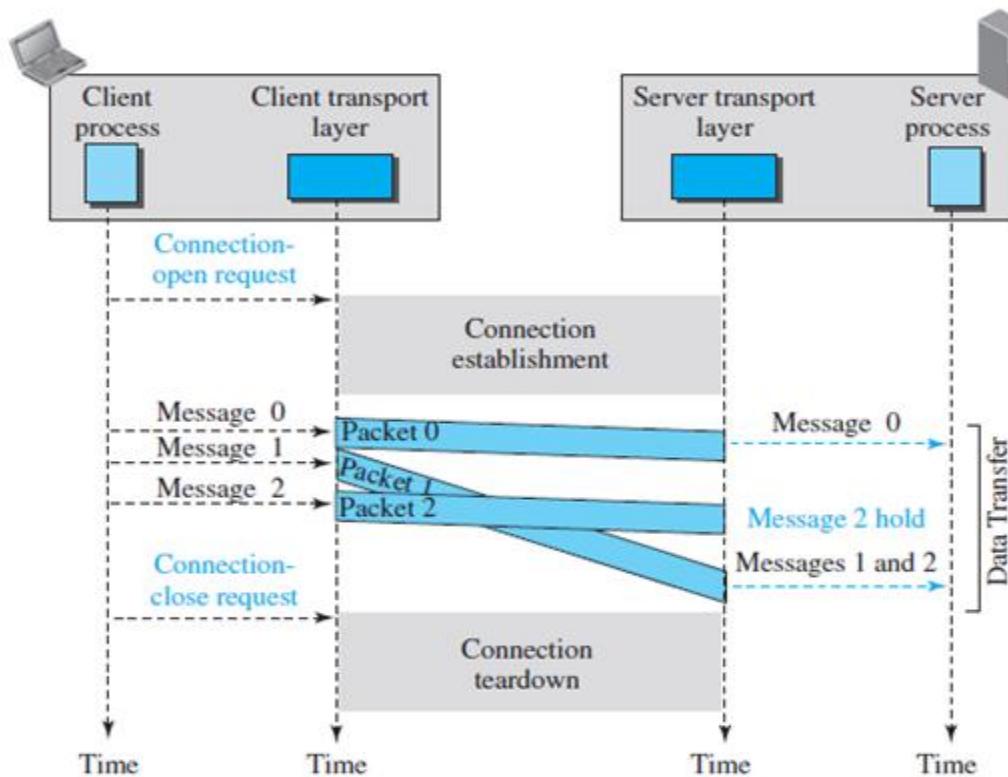
- In a connectionless service, the source process (application program) needs to divide its message into chunks of data of the size acceptable by the transport layer and deliver them to the transport layer one by one (Refer fig 2.6).



**Fig 2.6 – Connectionless service**

#### Connection-Oriented Service

- In a connection-oriented service, the client and the server first need to establish a logical connection between themselves.
- The data exchange can only happen after the connection establishment. After data exchange, the connection needs to be torn down (Refer fig 2.7)

**Fig 2.7 – Connection-oriented service**

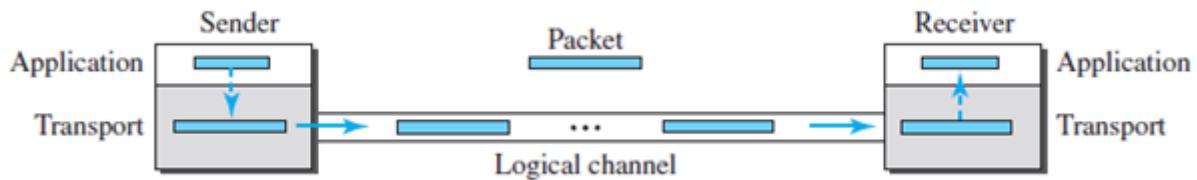
## 2. List & explain the protocols used in transport layer.

### Synopsis:

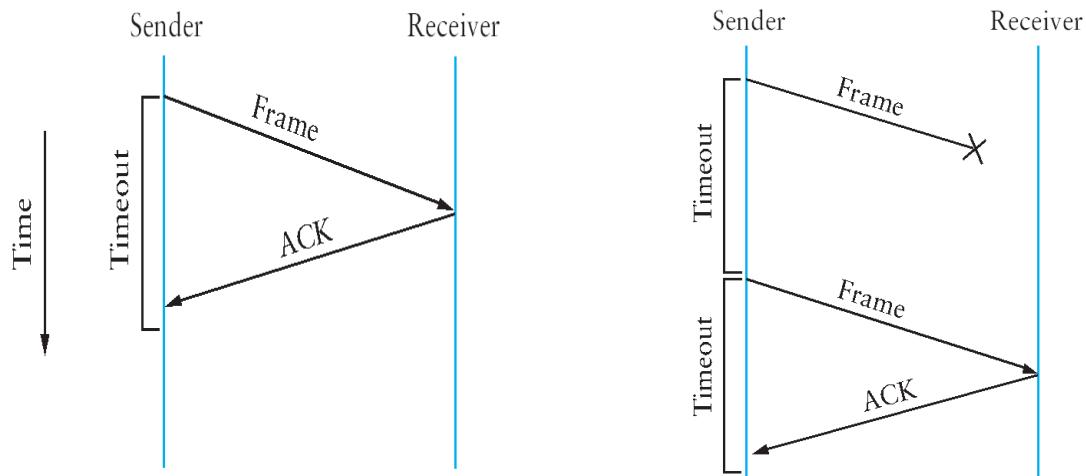
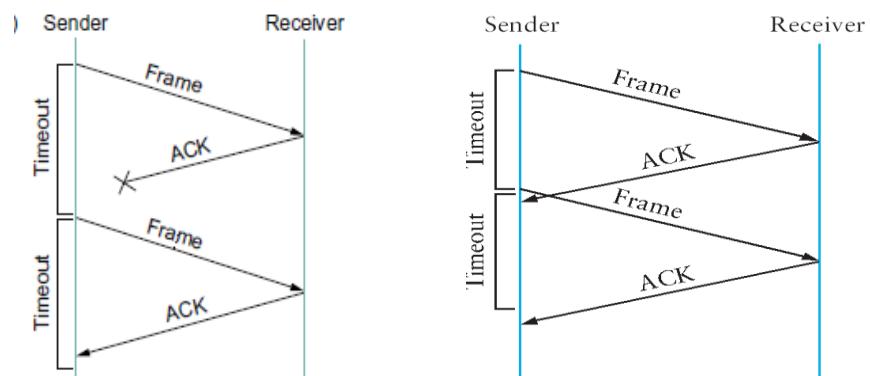
- **Simple Protocol**
- **Stop-and-Wait Protocol**
- **Go-Back-N Protocol (GBN)**
- **Selective-Repeat Protocol**
- **Bidirectional Protocols: Piggybacking**

### Simple Protocol

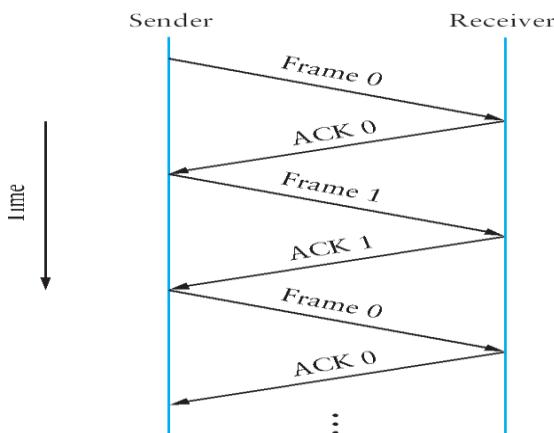
- Our first protocol is a simple connectionless protocol with neither flow nor error control.
- We assume that the receiver can immediately handle any packet it receives. In other words, the receiver can never be overwhelmed with incoming packets. (Refer fig 2.8).

**Fig 2.8 – Simple protocol****Stop and Wait Protocol**

- After transmitting one frame, **the sender waits for an acknowledgment before transmitting the next frame.**
- If the acknowledgment does not arrive after a certain period of time, the sender times out and retransmit the original frame.

**a) The ACK is received before the timer expires. b) The original frame is lost.****c) The ACK is lost****d) The timeout fires too soon****Fig 2.9 – Stop and Wait Protocol**

- Fig: illustrates four different scenarios that result from this basic algorithm. The sending side is represented on the left, the receiving side is depicted on the right, and time flows from top to bottom. (Refer fig 2.9).
- In Fig (a) ACK is received before the timer expires, (b) and (c) show the situation in which the original frame and the ACK, respectively, are lost, and (d) shows the situation in which the timeout fires too soon..
- Suppose the sender sends a frame and the receiver acknowledges it, but the acknowledgment is either lost or delayed in arriving. This situation is in (c) and (d). In both cases, the sender times out and retransmit the original frame, but the receiver will think that it is the next frame, since it correctly received and acknowledged the first frame.
- This makes the receiver to receive the duplicate copies. To avoid this two sequence numbers (0 and 1) must be used alternatively. (Refer fig 2.10).



**Fig 2.10 – Stop and Wait Protocol – Normal operation.**

- The main drawback of the stop-and-wait algorithm is that it allows the sender have only one outstanding frame on the link at a time.

### Sliding Window Protocol

- **The sender can transmit several frames before needing an acknowledgement.**
- Frames can be sent one right after another meaning that the link can carry several frames at once and its capacity can be used efficiently.
- The receiver acknowledges only some of the frames, using a single ACK to confirm the receipt of multiple data frames
- Sliding Window refers to imaginary boxes at both the sender and the receiver.
- Window can hold frames at either end and provides the upper limit on the number of frames that can be transmitted before requiring an acknowledgement.

- Frames are numbered modulo-n which means they are numbered from 0 to n-1.
- For eg. If n=8 the frames are numbered 0,1,2,3,4,5,6,7. i.e the size of the window is n -1.
- When the receiver sends ACK it includes the number of the next frame it expects to receive.
- When the sender sees an ACK with the number 5, it knows that all frames up through number 4 have been received.

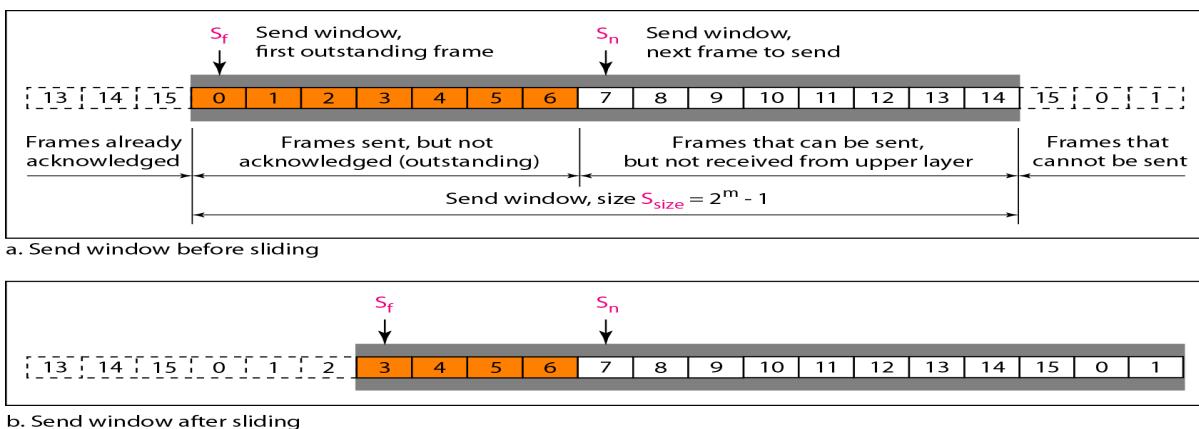
There are two methods to retransmit the lost frames

- GO-Back N
- Selective Repeat

### Go – Back N Protocol

#### Sender Window

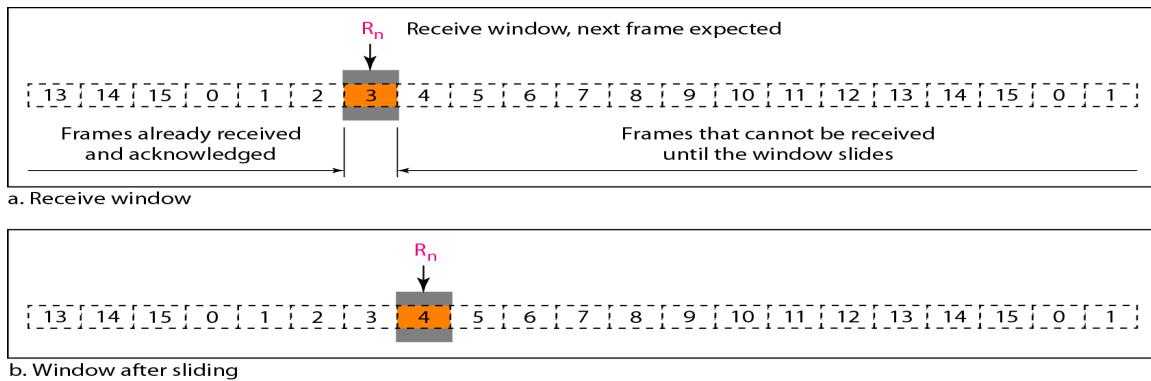
- At the beginning of transmission, the sender window contains n-1 frames. As frames are sent out, the left boundary of the window moves inward, shrinking the size of the window.
- If size of window is W if three frames have been transmitted since the last acknowledgement then the number of frames left in the window is w -3.
- Once an ACK arrives, the window expands to allow in a number of new frames equal to the number of frames acknowledged by that ACK. (Refer fig 2.11).



**Fig 2.11 – Go – Back N Protocol (sender window)**

#### Receiver Window

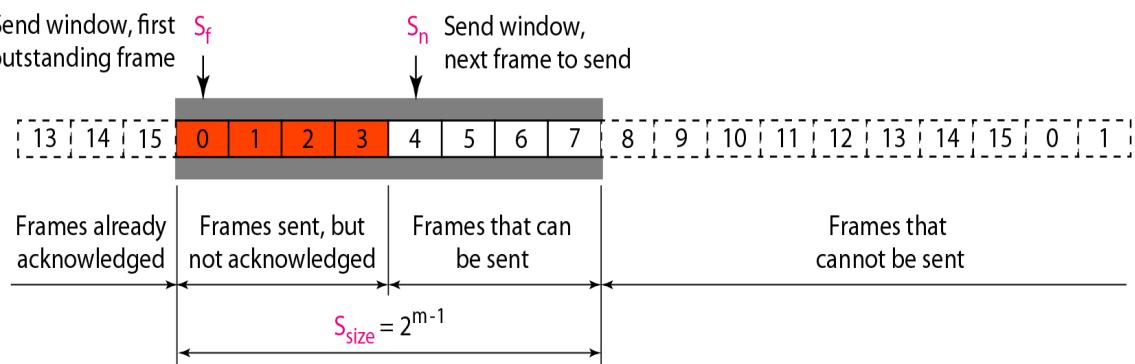
- The receive window is an abstract concept defining an imaginary box of size 1 with one single variable Rn.
- The window slides when a correct frame has arrived, sliding occurs one slot at a time.

**Fig 2.12 – Go – Back N Protocol (receiver window)**

- When the timer expires, the sender resends all outstanding frames. For example, suppose the sender has already sent frame 6, but the timer for frame 3 expires.
- This means that frame 3 has not been acknowledged; the sender goes back and sends frames 3, 4, 5, and 6 again. That is why the protocol is called *Go-Back-N*. (Refer fig 2.13).

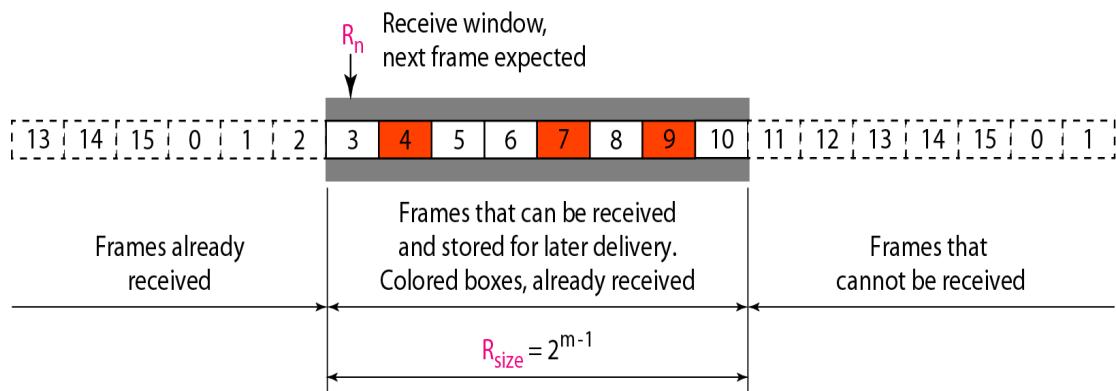
### Selective Repeat Protocol

#### Sender Window

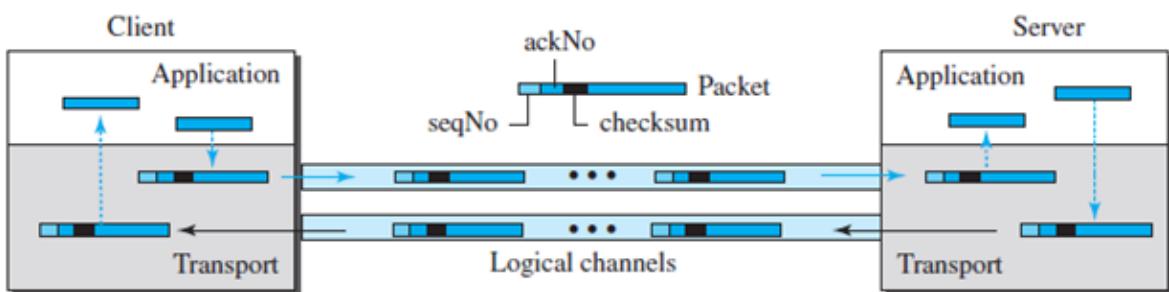
**Fig 2.13 – Selective repeat (sender window)**

#### Receiver window

- The Selective Repeat Protocol allows as many frames as the size of the receive window to arrive out of order and be kept until there is a set of in-order frames to be delivered to the network layer.
- Because the sizes of the send window and receive window are the same, all the frames in the send frame can arrive out of order and be stored until they can be delivered.
- If any frame lost, sender has to retransmit only that lost frames. (Refer fig 2.14).

**Fig 2.14– Selective repeat (receiver window)****Bidirectional Protocols: Piggybacking**

- The four protocols we discussed earlier in this section are all unidirectional: data packets flow in only one direction and acknowledgments travel in the other direction.
- In real life, data packets are normally flowing in both directions: from client to server and from server to client.
- This means that acknowledgments also need to flow in both directions.
- A technique called **piggybacking** is used to improve the efficiency of the bidirectional protocols.
- When a packet is carrying data from A to B, it can also carry acknowledgment feedback about arrived packets from B; when a packet is carrying data from B to A, it can also carry acknowledgment feedback about the arrived packets from A. (Refer fig 2.15).

**Fig 2.15– Piggybacking in Go-Back-N**

**3.Explain the working of USER DATAGRAM PROTOCOL (UDP) or Simple Demultiplexer (May 2016) (or) Explain the UDP header format & UDP applications (Nov 2021).**

### **Synopsis:**

- **Introduction**
- **Advantages**
- **Basic Properties of UDP (services)**
- **UDP Message Format**
- 

### **Introduction:**

- The UDP is called a **connection less, unreliable transport protocol**.
- The purpose of UDP is to **break up a stream of data into datagram**, add a source and destination port information, a length and a checksum.
- It is the receiving application's responsibility to detect and recover lost or damaged packets, as UDP doesn't take care of this.

### **Advantages:**

- It is a very simple protocol using a **minimum of overhead**.
- If a process wants to **send a small message** and doesn't care much about reliability, it can use UDP.
- It is a convenient protocol for multimedia and multicasting applications.
- Sending a small message by using UDP takes much less interaction between the sender and receiver than using TCP.

### **Basic Properties of UDP (services):**

- **UDP is a connectionless transport protocol.**
  - A UDP application sends messages without establishing and then closing a connection.
  - UDP has a smaller overhead than TCP, especially when the total size of the messages is small.

➤ **UDP does not guarantee reliable data delivery.**

- UDP messages can be lost or duplicated, or they may arrive out of order; and they can arrive faster than the receiver can process them.
- The application programmers using UDP have to consider and tackle these issues themselves.
- Not buffered -- UDP accepts data and transmits immediately (no buffering before transmission).
- Full duplex -- concurrent transfers can take place in both directions.

➤ **UDP has no mechanism for flow control.**

➤ **Multiplexing and Demultiplexing.**

- This is many to one relationship used in sender side.
- The protocol accepts messages from different processes, differentiated by their assigned port numbers.
- Demultiplexing is one to many relationship used in receiver side.

➤ **Encapsulation and Decapsulation.**

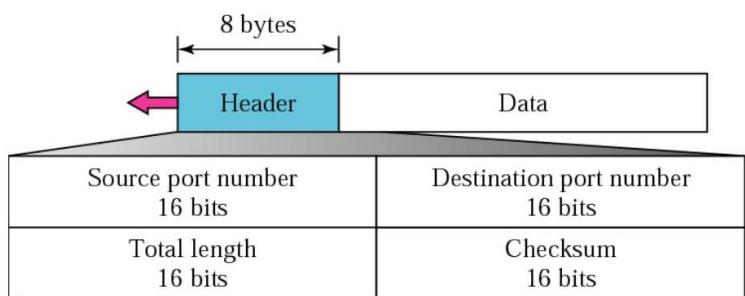
- To send a message from one processes to another, the UDP protocol encapsulate and decapsulate messages in an IP datagram.
- Encapsulate each UDP message in an IP datagram, and use IP to deliver this datagram across the internet.

### **UDP Message Format**

#### **User Datagram:**

- UDP packets called **user datagram** which has a fixed size header of 8 bytes. (Refer fig 2.16).

#### **Format of User Datagram:**



**Fig 2.16– UDP Header format**

User datagram has the following fields.

➤ **Source Port Number**

- The source port number used by the processes running on the **source host** (local computer).

- It is 16 bits long, which means that the port number can range from 0 to 65535. If the source host is the client, the port number requested by the processes and chosen by the UDP software running on the source host.

➤ **Destination Port Number**

- This is the port number used by the processes running on the **destination host**.
- It is also 16 bits long. The Destination port is usually a 'well known' port number such as 69 for trivial file transfer protocol, or 53 for DNS.
- These port numbers allow the remote machine to recognize a request for a particular type of service. If the destination host is a client, the server copies the port number it has received in the request packet.

➤ **Length**

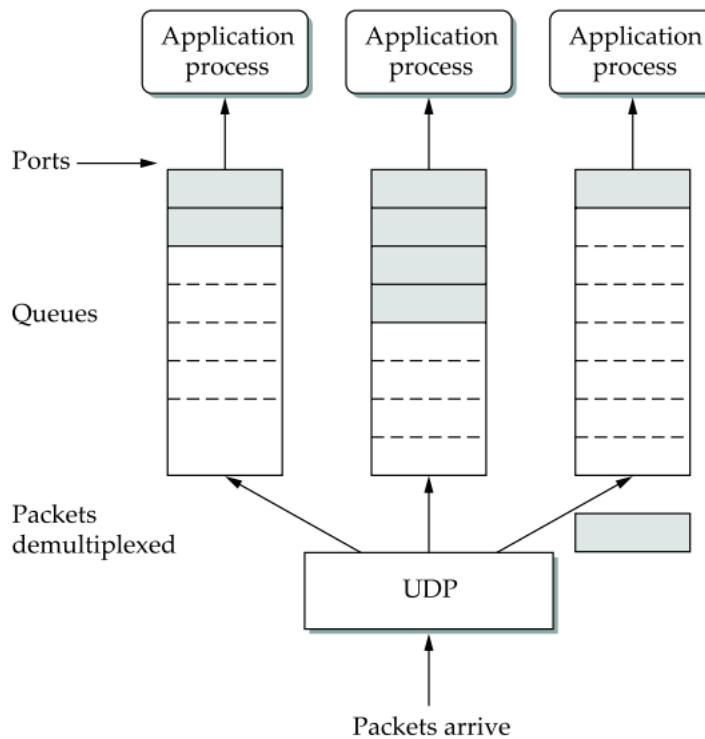
- This is a 16 bits field that defines the **total length of the user data gram**, header plus data. The 16 bits can define a total length of 0 to 65535 bytes.

➤ **Checksum**

- This field is used to **detect errors** over the entire user datagram.
- The calculation of checksum and its inclusion in the user datagram are optional.

**Process communication in UDP**

- The next issue is how a process learns the port for the process to which it wants to send the message. (Refer fig 2.17).
- **Typically a client process initiates a message exchange with a server process. Once a client has contacted a server, the server knows the client's port (it was contained in the message header) and can reply to it.**
- The real problem, therefore, is how the client learns the server's port in the first place. A common approach is for the server to accept messages at a well known port.
- That is, each **server receives its messages at some fixed port that is widely published, much like the emergency telephone service available at the well-known number 911.**
- In the Internet, for example, the domain name server (DNS) receives messages at well-known port 53 on each host, the mail service listens of messages at port 25, and the Unix talk program accepts messages at well known port 517, and so on.

**Fig 2.17 – UDP Message queue**

- This mapping is published periodically in an RFC and is available on the most Unix systems in file /etc/services. Sometimes a well-known port to agree on some other port that they will use for subsequent communication leaving the well-known port free for other clients.
- A port is purely an abstraction. Exactly how it is implemented differs from system to system, or more precisely, from OS to OS.
- **For example,** the socket API is an example implementation of ports.
  - Typically, a port is implemented by a message queue.
  - When a message arrives, the protocol (eg. UDP) appends the message to the end of the queue. Should the queue be full, the message is discarded.
- There is no flow-control mechanism that tells the sender to slow down. When an application process wants to receive a message, one is removed from the front of the queue. If the queue is empty, the process blocks until a message becomes available.

#### **Uses or applications of UDP**

- UDP is used for process with simple request-response communication with little concern for and error control.
- UDP is suitable for a process with internal flow and error control mechanism.

- UDP is suitable for multicasting. Multicasting capabilities are embedded in UDP software but not in TCP software.
- UDP is used for some route updating protocols, such as routing information protocol (RIP).
- UDP is used for management processes such as SNMP.

### **Difference between TCP and UDP**

- TCP is a connection-oriented protocol, whereas UDP is a connectionless protocol.
- A key difference between TCP and UDP is speed, as TCP is comparatively slower than UDP. Overall, UDP is a much faster, simpler, and efficient protocol, however, retransmission of lost data packets is only possible with TCP.

#### **4. Describe in detail about TCP segment (Header) format (NOV 2013, 2014)**

**(May & Nov 2015) (or) Draw the format of TCP Packet header and explain each of its field and Specify the justification for having variable field length for the field in TCP header. Apr 2017 (Nov 2021).**

#### **Synopsis:**

- **Introduction**
- **TCP Header format**

#### **Introduction:**

- A Packet in TCP is called a segment. The below diagram shows the format of the segment.
- The segment consists of a 20 to 60 byte header, followed by data from the application program. The header is 20 bytes if there are no options and up to 60 bytes if it contains options. (Refer fig 2.18).

#### **TCP Header format:**

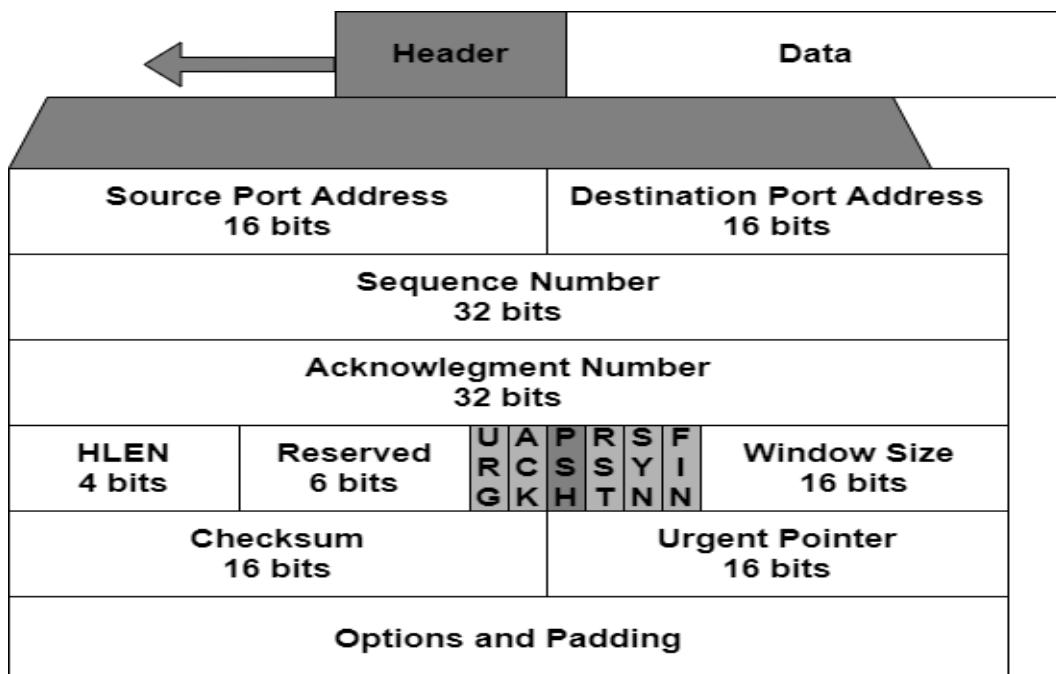
- **Header**
  - The header is composed of a 20-byte fixed part and an optional part with a variable length. The total size of the header (in 32-bit words) is specified in HLEN.
- **Data**
  - The data can have a variable size, which can be up to  $65535 - 20 = 65515$  bytes.

➤ **Source port number (16 bits)**

- The SOURCE PORT field identifies the TCP process which sent the datagram.

➤ **Destination port number (16 bits)**

The DESTINATION PORT field identifies the TCP process which is receiving the datagram.



**Fig 2.18 – TCP Header format**

➤ **Sequence number (32 bits)**

- The SEQUENCE NUMBER field identifies the first byte of the outgoing data. The receiver uses this to re-order segments arriving out of order and to compute an acknowledgement number.

➤ **Acknowledgement number (32 bits)**

- Contains the next sequence number that the sender of the acknowledgement expects to receive which is the sequence number plus 1 (plus the number of bytes received in the last message). This number is used only if the ACK flag is on. The ACKNOWLEDGEMENT NUMBER field identifies the sequence number of the incoming data that is expected next.

➤ **Header Length**

- This 4-bit field indicates the number of 4-byte words in the TCP header. The length of the header can be between 20 and 60 bytes.

➤ **Reserved**

- This is a 6-bit field reserved for future use.

➤ **Code bits**

- The CODE BITS (*or FLAGS*) field contains one or more 1-bit flags
- Control bits to indicate end of stream, acknowledgement field being valid, connection reset, urgent pointer field being valid, etc.

**Table 2.2 – Code bits**

<b>[CONTROL]: URG (1)-</b>	Urgent Bit validates the Urgent Pointer field.
<b>[CONTROL]: ACK (1)-</b>	Acknowledge Bit, set if the Acknowledge Number field is being used
<b>[CONTROL]: PSH (1)-</b>	Push Bit tells the sender that a higher throughput is required.
<b>[CONTROL]: RST (1)-</b>	Reset Bit resets the connection when there's conflicting sequence numbers.
<b>[CONTROL]: SYN (1)-</b>	Sequence Number Synchronization. Used in 3 types of segments: connection request, connection confirmations (with ACK) and confirmation termination (with FIN) in 3 types of segments: terminal request, terminal confirmation (with ACK) and acknowledgement of terminal confirmation (with ACK).
<b>[CONTROL]: FIN (1)-</b>	Used with SYN to confirm termination of connections

➤ **Window Size(16 bit)**

- The **WINDOW** field identifies how much buffer space is available for incoming data.
- During piggybacking, how much data a receiver is willing to accept.

**Note:** The process of sending data along with the acknowledgment is called **piggybacking**.

➤ **Checksum(16 bit)**

- The **CHECKSUM** field contains a simple checksum over the TCP segment header and data.

➤ **Urgent Pointer (16 bit)**

- This 16-bit field, which is valid only if the urgent flag is set, is used when the segment contains urgent data. It defines the number that must be added to the sequence number to obtain the number of the last urgent byte in the data section of the segment.

➤ **Options**

- There can be up to 40 bytes of optional information in the TCP header.

- 5. Explain in detail about TCP connection establishment & termination (TCP Connection Management) (NOV 2013) (May & Nov 2015) Nov 2017 (or) Demonstrate how TCP three-way handshake works (Nov 2021).**

**Synopsis:**

- **Introduction**
- **Connection establishment**
- **Three-way handshaking**
- **Data Transfer**
- **Pushing Data**
- **TCP Connection Release (or) Connection Termination**
- **Three-way handshaking**
- **TCP Connection Management (State transition diagram)**
- **Client Diagram**
- **Server Diagram**

#### **Introduction:**

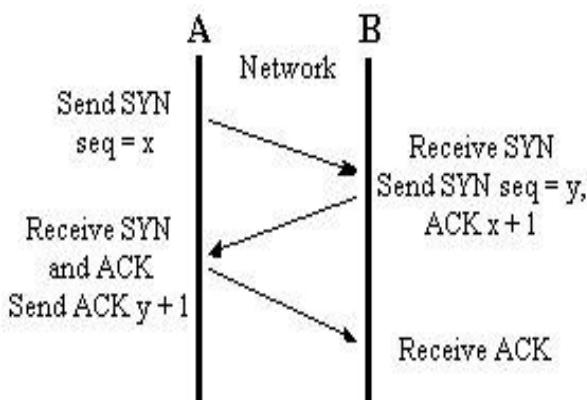
- **TCP is connection-oriented.** A connection-oriented transport protocol establishes a virtual path between the source and destination.
- All the segments belonging to a message are then sent over this virtual path.
- Using a single virtual pathway for the entire message facilitates the **acknowledgement process as well as retransmission of damaged or lost frames.** TCP, which uses the services of IP, a connection-less protocol, can be connection-oriented.
- TCP uses the services of IP to deliver individual segments to the receiver, but it controls the connection itself. If a segment is lost or corrupted, it is retransmitted.
- In TCP connection-oriented transmission requires two phases:
  - ✓ Connection establishment and Data transfer.
  - ✓ Connection termination.

#### **Connection establishment:**

- TCP transmits data in full-duplex mode. When two TCP's in two machines or connected, they are able to send segments to each other simultaneously.

***Three-way handshaking.***

- The connection establishment in TCP is called three way handshaking.
- **The process starts with the server. The server program tells its TCP that it is ready to accept a connection. This is called a request for a passive open.** (Refer fig 2.19).
- **The client program issues a request for an active open.** A client that wishes to connect to an open server tells its TCP that it needs to be connected to that particular server. TCP can now start the three-way handshaking process. Each segment has the sequence number the acknowledgement number, the control flags, and the window size, if not empty.

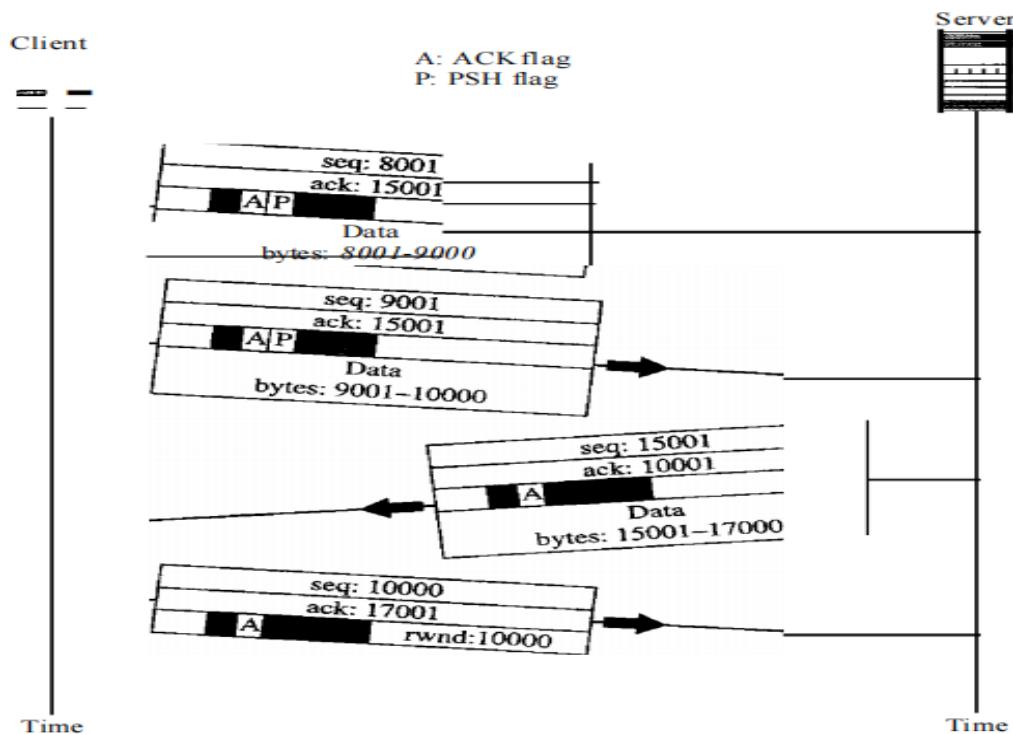
**Fig 2.19 – Connection establishment**

**The three steps in this phase are as follows.**

1. The client sends the first segment, a **SYN segment**, in which only the SYN flag is set. This segment is for synchronization of sequence numbers. It consumes one sequence number. When the data transfer starts, the sequence number is incremented by 1. A SYN segment cannot carry data, but it consumes one sequence number.
2. The server sends the second segment, a **SYN + ACK segment**, with 2 flag bits set: SYN and ACK. This segment has a dual purpose. It is a SYN segment for communication in the other direction and serves as the acknowledgement for the SYN segment. It consumes one sequence number.
3. The client sends the third segment. This is just an **ACK segment**. It acknowledges the receipt of the second segment with the ACK flag and acknowledgement number field.

## Data Transfer

- After connection is established, bidirectional data transfer can take place. The client and server can both send data and acknowledgements. (Refer fig 2.20).
- The below figure shows an example. In this example, after connection is established, the client sends 2000 bytes of data in two segments. The server then sends 2000 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 acknowledgement because there are no more data to be sent.
- The data segments sent by the client have the PSH (push) flag set so that the server TCP knows to deliver data to the server process as soon as they are received.



**Fig 2.20 – Data transfer**

### Pushing Data:

- The sending TCP uses a buffer to store the stream of data coming from the sending application program.
- The sending TCP can select the segment size. The receiving TCP also buffers the data when they arrive and delivers them to the application program when

the application program is ready or when it is convenient for the receiving TCP. **This type of flexibility increases the efficiency of TCP.**

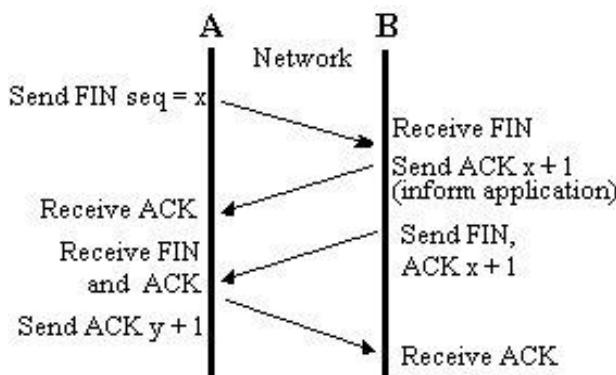
- The application program at the sending site can request a push operation.
- This means that the sending TCP must not wait for the window to be filled.
- It must create a segment and send it immediately.
- The sending TCP must also set the push bit (PSH) to let the receiving TCP know that the segment includes data that must be delivered to the receiving application program as soon as possible and not to wait for more data to come.

### TCP Connection Release (or) Connection Termination

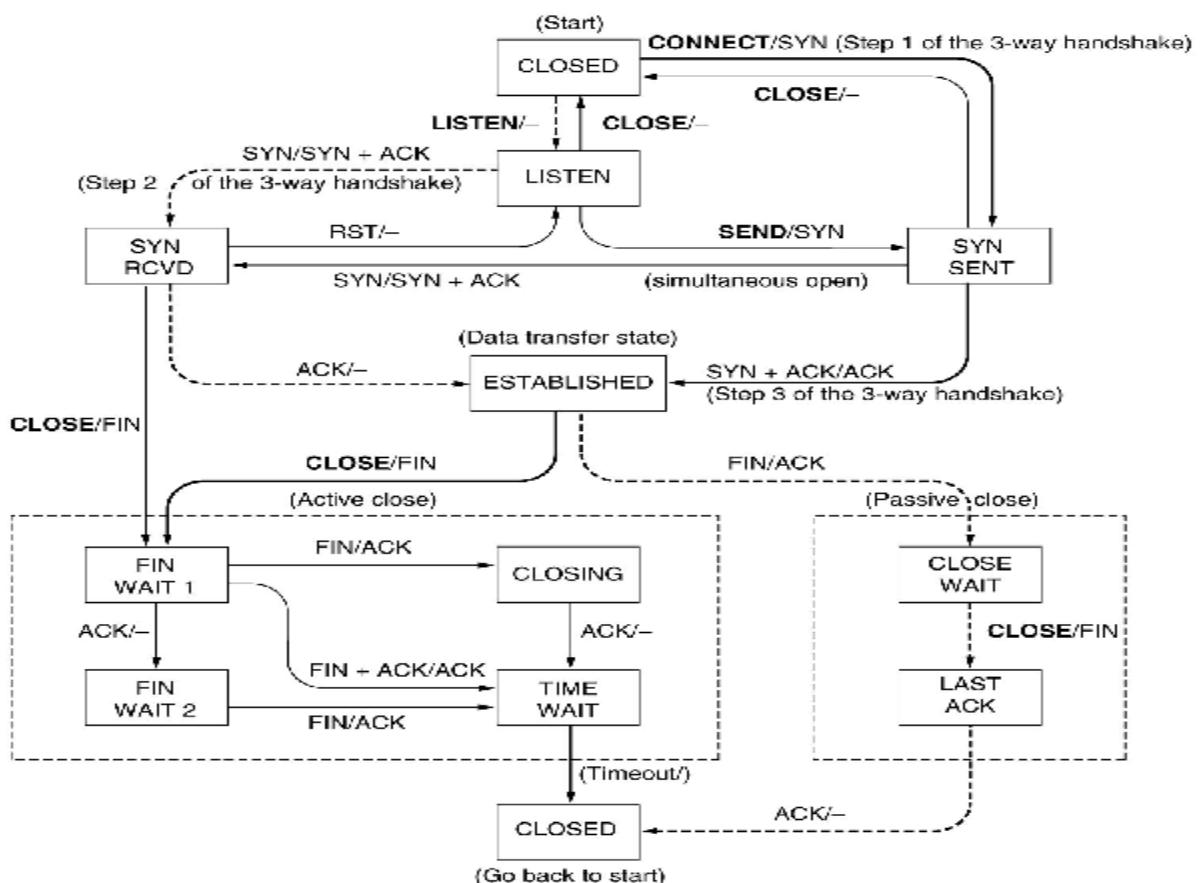
- Any of the two parties involved in exchanging data (client or server) can close the connection, although it is usually initiated by the client.
- Most implementations today allow two options for connection termination: three-way handshaking and four-way handshaking with a half-close option.

#### *Three-way handshaking*

- In a normal 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. (Refer fig 2.21)
1. 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. The FIN + ACK segment consumes one sequence number if it does not carry data.
  2. 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 acknowledgement number, which is 1 plus the sequence number received in the FIN segment from the server. This segment cannot carry data and consumes no sequence number.

**Fig 2.21 – Connection Termination****TCP Connection Management (State transition diagram) (NOV/DEC 2013).**

- The steps to manage a TCP connection can be represented in a finite state machine with the eleven states listed in Figure 2.22

**Fig 2.22 – State transition diagram**

State	Description
CLOSED	No connection is active or pending
LISTEN	The server is waiting for an incoming call
SYN RCVD	A connection request has arrived; wait for ACK
SYN SENT	The application has started to open a connection
ESTABLISHED	The normal data transfer state
FIN WAIT 1	The application has said it is finished
FIN WAIT 2	The other side has agreed to release
TIMED WAIT	Wait for all packets to die off
CLOSING	Both sides have tried to close simultaneously
CLOSE WAIT	The other side has initiated a release
LAST ACK	Wait for all packets to die off

**Table 2.3 - States*****Client Diagram:***

- The client TCP starts in the CLOSED state.
- While in this state, the client TCP can receive an active open request from the client application program. It sends a SYN segment to the server TCP and goes to the SYN-SENT state.
- While in this state, the client TCP can receive a SYN + ACK segment from other TCP. It sends an ACK segment to the other TCP and goes to the ESTABLISHED state. This is the data transfer state. The client remains in this state as long as it is sending and receiving data.
- While in this state, the client TCP can receive a close request from the client application program. It sends a FIN segment to the other TCP and goes to the FIN-WAIT1 state.
- While in this state, the client TCP waits to receive an ACK from the server TCP. When ACK is received, it goes to the FIN-WAIT2 state. Now the connection is closed in one direction.
- The client remains in this state, waiting for the server to close the connection. If it receives a FIN segment, it sends an ACK segment and goes to the TIME-WAIT state.
- When the client is in this state, it starts a timer and waits until this timer goes off. After the time-out, the client goes to the CLOSED state, where it began.

***Server Diagram:***

- The server TCP starts in the CLOSED state.
- While in this state, the server TCP can receive an open request from the server application program, it goes to the LISTEN state.
- While in this state, the server TCP can receive a SYN segment. It sends a SYN + ACK segment to the client and goes to the SYN-RCVD state.
- While in this state, the server TCP receives an ACK and goes to ESTABLISHED state. This is the data transfer state. The server remains in this state as long as it is receiving and sending data.
- While in this state, the server TCP can receive a FIN segment from the client. It can send an ACK and goes to the CLOSE-WAIT state.
- While in this state, the server waits until it receives a close request from the server program. It then sends a FIN segment and goes to LAST-ACK state.
- While in this state, the server waits for the last ACK segment and goes to the CLOSED state.

**6. Discuss TCP Services & Features****Transmission Control Protocol (TCP):****Synopsis:**

- **Definition**
- **TCP Services**
  - **Stream Delivery Service**
  - **Sending and Receiving Buffers**
  - **Full-Duplex Communication**
  - **Multiplexing and Demultiplexing**
  - **Connection-Oriented Service**
  - **Reliable Service**
- **TCP Features**
- **Windows in TCP**
  - **Send Window**
  - **Receive Window**

**Definition:**

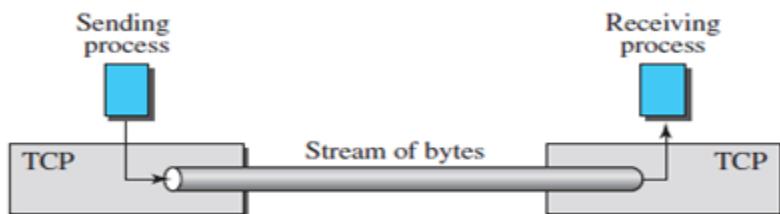
- **Transmission Control Protocol (TCP)** is a connection-oriented, reliable protocol.
- TCP explicitly defines connection establishment, data transfer, and connection teardown phases to provide a connection-oriented service.

## TCP Services

### Process-to-Process Communication

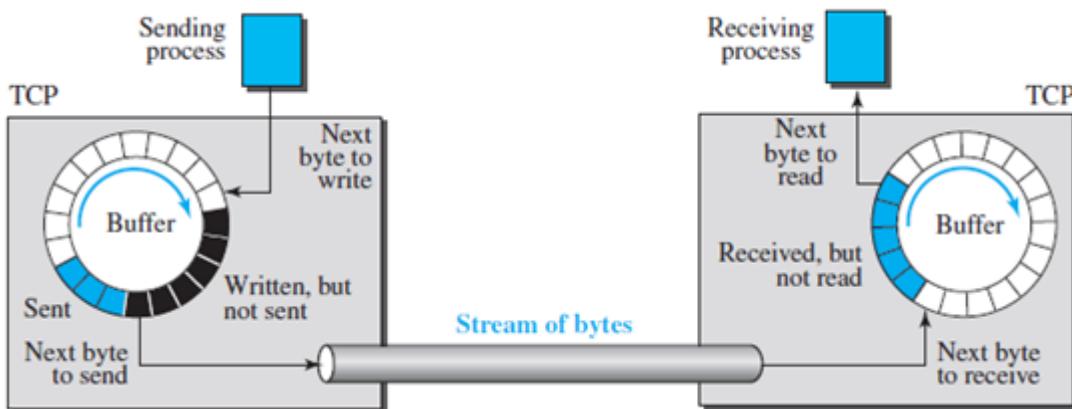
- As with UDP, TCP provides process-to-process communication using port numbers.

### Stream Delivery Service



**Fig 2.23 – Stream Delivery**

### Sending and Receiving Buffers



**Fig 2.24 – Sending and Receiving Buffers**

### Full-Duplex Communication

- TCP offers *full-duplex service*, where data can flow in both directions at the same time.
- Each TCP endpoint then has its own sending and receiving buffer, and segments move in both directions.

### Multiplexing and Demultiplexing

- Like UDP, TCP performs multiplexing at the sender and demultiplexing at the receiver.
- However, since TCP is a connection-oriented protocol, a connection needs to be established for each pair of processes.

### Connection-Oriented Service

- TCP, unlike UDP, is a **connection-oriented protocol**.
- When a process at site A wants to send to and receive data from another process at site B, the following three phases occur:
  1. The two TCP's establish a logical connection between them.
  2. Data are exchanged in both directions.
  3. The connection is terminated.

### Reliable Service

- TCP is a **reliable transport protocol**.
- It uses an acknowledgment mechanism to check the safe and sound arrival of data. We will discuss this feature further in the section on error control.

### TCP Features

- *Numbering System*
- *Byte Number*
- *Sequence Number*
- *Acknowledgment Number*

### Windows in TCP:

#### Send Window

- The sender maintains three variables:
  - ✓ The **send window size**, denoted **SWS**, gives the upper bound on the number of outstanding (unacknowledged) frames that the sender can transmit;
  - ✓ **LAR** denotes the sequence number of the **last acknowledgment received**; and
  - ✓ **LFS** denotes the sequence number of the **last frame sent**.
- The sender also maintains the following invariant:

$$\boxed{\mathbf{LFS-LAR \leq SWS}}$$

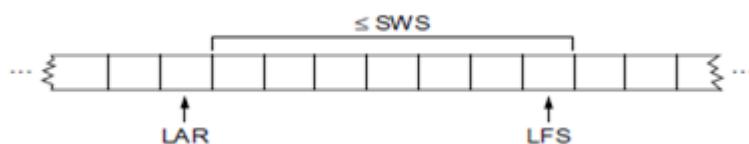
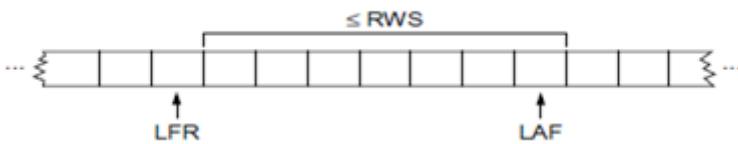
- When an acknowledgment arrives, the sender moves LAR to the right, thereby, allowing the sender to transmit another frame.
- Also, the sender associates a timer with each frame it transmits, and it retransmits the frame should the timer expire before an ACK is received.
- Notice that the sender has to be willing to buffer up to SWS frames since it must be prepared to retransmit them until they are acknowledged.

#### Receive Window

- The receiver maintains the following three variables: (Refer fig 2.25)

- ✓ The **receive window size**, denoted **RWS**, gives the upper bound on the number of out-of-order frames that the receiver is willing to accept;
  - ✓ LAF denotes the sequence number of the **largest acceptable frame**; and
  - ✓ LFR denotes the sequence number of the **last frame received**.
- The receiver also maintains the following invariant (Refer fig 2.26)

$$\text{LAF} - \text{LFR} \leq \text{RWS}$$

**Fig 2.25 – Sliding window on sender****Fig 2.26 – Sliding window on receiver**

- When a frame with sequence number SeqNum arrives, the receiver takes the following action.
  1. If  $\text{SeqNum} \leq \text{LFR}$  or  $\text{SeqNum} > \text{LAF}$ , then the frame is outside the receiver's window and it is discarded.
  2. If  $\text{LFR} < \text{SeqNum} \leq \text{LAF}$ , then the frame is within the receiver's window and it is accepted.
  3. Now the receiver needs to decide whether or not to send an ACK. Let  $\text{SeqNumToAck}$  denote the largest sequence number not yet acknowledged, such that all frames with sequence numbers less than or equal to  $\text{SeqNumToAck}$  have been received.
  4. The receiver acknowledges the receipt of  $\text{SeqNumToAck}$ , even if higher numbered packets have been received. This acknowledgment is said to be cumulative. It then sets  $\text{LFR} = \text{SeqNumToAck}$  and adjusts  $\text{LAF} = \text{LFR} + \text{RWS}$ .

**7. Explain in detail about TCP flow control OR TCP Adaptive flow control  
(NOV/DEC 2013, 2014) APR 2017. (April/may 2023) (April/may 2024)**

**Synopsis:**

- **Definition**
- **Reliable and Ordered Delivery**
- **Flow Control**

**Definition:**

- TCP uses a sliding *window* mechanism to control the flow of data. When a connection is established, each end of the connection allocates a buffer to hold incoming data, and sends the size of the buffer to the other end.
- As data arrives, the receiver sends acknowledgements together with the amount of buffer space available called a **window advertisement**.
- Sliding window algorithm serves several purposes.
  1. It guarantees the reliable delivery of data
  2. It ensures that data is delivered in order.
  3. It enforces flow control between, the sender and the receiver.

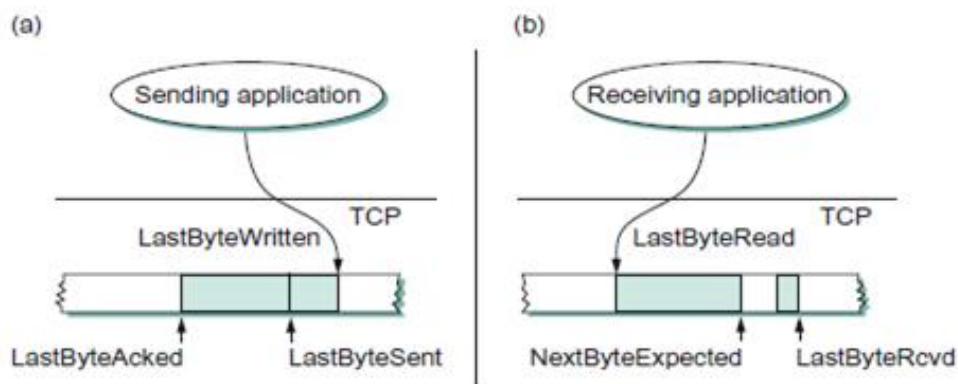
**Reliable and Ordered Delivery**

- To see how the sending and receiving sides of TCP interact with each other to implement reliable and ordered delivery, consider the situation illustrated in Figure 5.8.
- **TCP on the sending side maintains a send buffer.**
- This buffer is used to store data that has been sent but not yet acknowledged, as well as data that has been written by the sending application but not transmitted.
- **On the receiving side, TCP maintains a receive buffer.**
- This buffer holds data that arrives out of order, as well as data that is in the correct order (i.e., there are no missing bytes earlier in the stream) but that the application process has not yet had the chance to read.
- To make the following discussion simpler to follow, we initially ignore the fact that both the buffers and the sequence numbers are of some finite size and hence will eventually wrap around.
- Also, we do not distinguish between a pointer into a buffer where a particular byte of data is stored and the sequence number for that byte.
- Looking first at the sending side, three pointers are maintained into the send buffer, each with an obvious meaning: LastByteAcked, LastByteSent, and LastByteWritten. Clearly,

**LastByteAcked  $\leq$  LastByteSent**

since the receiver cannot have acknowledged a byte that has not yet been sent, and

**LastByteSent  $\leq$  LastByteWritten**



**Fig 2.27 – Relationship between TCP a) Send buffer, b) Receive buffer**

- since TCP cannot send a byte that the application process has not yet written.
- Also note that none of the bytes to the left of LastByteAcked need to be saved in the buffer because they have already been acknowledged, and none of the bytes to the right of LastByteWritten need to be buffered because they have not yet been generated. (Refer fig 2.27).
- A similar set of pointers (sequence numbers) are maintained on the receiving side: LastByteRead, NextByteExpected, and LastByteRcvd. The inequalities are a little less intuitive, however, because of the problem of out-of-order delivery. The first relationship

**LastByteRead < NextByteExpected**

is true because a byte cannot be read by the application until it is received and all preceding bytes have also been received.

- NextByteExpected points to the byte immediately after the latest byte to meet this criterion. Second,

$$\text{NextByteExpected} \leq \text{LastByteRcvd} + 1$$

- since, if data has arrived in order, NextByteExpected points to the byte after LastByteRcvd, whereas if data has arrived out of order, then NextByteExpected points to the start of the first gap in the data, as in Figure 4.27.
- Note that bytes to the left of LastByteRead need not be buffered because they have already been read by the local application process, and bytes to the right of LastByteRcvd need not be buffered because they have not yet arrived.

### Flow Control

- Recall that in a sliding window protocol, the size of the window sets the amount of data that can be sent without waiting for acknowledgment from the receiver.
- Thus, the receiver throttles the sender by advertising a window that is no larger than the amount of data that it can buffer. Observe that TCP on the receive side must keep,

$$\text{LastByteRcvd} - \text{LastByteRead} \leq \text{MaxRcvBuffer}$$

to avoid overflowing its buffer.

- It therefore advertises a window size of,

$$\text{AdvertisedWindow} = \text{MaxRcvBuffer} - (\text{NextByteExpected} - 1) - \text{LastByteRead}$$

which represents the amount of free space remaining in its buffer.

- As data arrives, the receiver acknowledges it as long as all the preceding bytes have also arrived.
- In addition, LastByteRcvd moves to the right (is incremented), meaning that the advertised window potentially shrinks.
- Whether or not it shrinks depends on how fast the local application process is consuming data. If the local process is reading data just as fast as it arrives (causing LastByteRead to be incremented at the same rate as LastByteRcvd), then the advertised window stays open (i.e., AdvertisedWindow = MaxRcvBuffer).
- If, however, the receiving process falls behind, perhaps because it performs a very expensive operation on each byte of data that it reads, then the advertised

window grows smaller with every segment that arrives, until it eventually goes to 0.

- TCP on the send side must then adhere to the advertised window it gets from the receiver. This means that at any given time, it must ensure that

$$\text{LastByteSent} - \text{LastByteAcked} \leq \text{AdvertisedWindow}$$

Said another way, the sender computes an *effective* window that limits how much data it can send:

$$\text{Effective Window} = \text{AdvertisedWindow} - (\text{LastByteSent} - \text{Last Byte Acked})$$

- All the while this is going on, the send side must also make sure that the local application process does not overflow the send buffer—that is, that

$$\text{LastByteWritten} - \text{LastByteAcked} \leq \text{MaxSendBuffer}$$

- If the sending process tries to write  $y$  bytes to TCP, but

$$(\text{LastByteWritten} - \text{LastByteAcked}) + y > \text{MaxSendBuffer}$$

then TCP blocks the sending process and does not allow it to generate more data.

## 8. Discuss TCP adaptive retransmission (APR 2017).

### Synopsis:

- TCP Adaptive Retransmission
- Original Algorithm
- Karn/Partridge Algorithm
- Jacobson/Karels Algorithm

### TCP Adaptive Retransmission:

- TCP copies with the loss of packets using a technique called **retransmission**.
- When TCP data arrives an *acknowledgement* is sent back to the sender. Whenever a TCP segment is transmitted, a copy of it is also placed on the **retransmission queue**.
- When TCP data is sent, a timer is started this starts from a particular value and counts down to zero. If the timer expires before an acknowledgement arrives, TCP retransmits the data.

- Three algorithm of adaptive retransmission
  - ✓ Simple algorithm (Original algorithm)
  - ✓ Kern/Partridge algorithm
  - ✓ Jacobson/Karels algorithm

### **Original Algorithm:**

- We begin with a simple algorithm for **computing a timeout value between a pair of hosts.**
- This is the algorithm that was originally described in the TCP specification—and the following description presents it in those terms—but it could be used by any end-to-end protocol.
- The idea is to keep a running average of the RTT and then to compute the timeout as a function of this RTT.
- Specifically, every time TCP sends a data segment, it records the time. When an ACK for that segment arrives, TCP reads the time again, and then takes the difference between these two times as a **SampleRTT**. TCP then computes an EstimatedRTT as a weighted average between the previous estimate and this new sample. That is,

$$\text{EstimatedRTT} = \alpha \times \text{EstimatedRTT} + (1 - \alpha) \times \text{SampleRTT}$$

- The parameter  $\alpha$  is selected to *smooth* the EstimatedRTT.
- A small  $\alpha$  tracks changes in the RTT but is perhaps too heavily influenced by temporary fluctuations.
- On the other hand, a large  $\alpha$  is more stable but perhaps not quick enough to adapt to real changes.
- The original TCP specification recommended a setting of  $\alpha$  between 0.8 and 0.9. TCP then uses EstimatedRTT to compute the timeout in a rather conservative way:

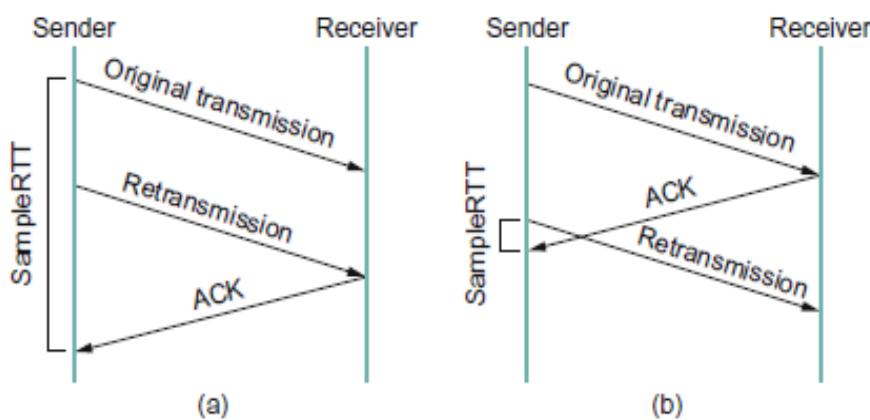
$$\text{Time Out} = 2 \times \text{EstimatedRTT}$$

### **Karn/Partridge Algorithm:**

- After several years of use on the Internet, a rather obvious flaw was discovered in this simple algorithm.
- The problem was that an ACK does not really acknowledge a transmission; it actually acknowledges the receipt of data.
- In other words, whenever a segment is retransmitted and then an ACK arrives at the sender, **it is impossible to determine if this ACK should be associated with the**

**first or the second transmission of the segment for the purpose of measuring the sample RTT.**

- It is necessary to know which transmission to associate it with so as to **compute an accurate SampleRTT**.
- As illustrated in Figure 4.38, if you assume that the ACK is for the original transmission but it was really for the second, then the SampleRTT is too large (a); if you assume that the ACK is for the second transmission but it was actually for the first, then the SampleRTT is too small (b).
- The solution, which was proposed in 1987, is surprisingly simple.
- **Whenever TCP retransmits a segment, it stops taking samples of the RTT; it only measures SampleRTT for segments that have been sent only once. This solution is known as the Karn/Partridge algorithm**, after its inventors.
- Their proposed fix also includes a second small change to TCP's timeout mechanism.
- Each time TCP retransmits, it sets the next timeout to be twice the last timeout, rather than basing it on the last EstimatedRTT.
- That is, Karn and Partridge proposed that TCP use **exponential backoff**, similar to what the Ethernet does.
- The motivation for using exponential backoff is simple: Congestion is the most likely cause of lost segments, meaning that the TCP source should not react too aggressively to a timeout.
- In fact, the more times the connection times out, the more cautious the source should become (Refer fig 2.28).



**Fig 2.28 – Associating the ACK with a) Original transmission, b) Retransmission**

**Jacobson/Karels Algorithm:**

- The Karn/Partridge algorithm was introduced at a time when the Internet was suffering from high levels of network congestion.
  - Their approach was designed to fix some of the causes of that congestion, but, although it was an improvement, the congestion was not eliminated.
  - The following year (1988), two other researchers—Jacobson and Karels—proposed a more drastic change to TCP to battle congestion.
  - The bulk of that proposed change is described in [Chapter 6](#). Here, we focus on the aspect of that proposal that is related to deciding when to time out and retransmit a segment.
  - As an aside, it should be clear how the timeout mechanism is related to congestion—if you time out too soon, you may unnecessarily retransmit a segment, which only adds to the load on the network.
  - The other reason for needing an accurate timeout value is that a timeout is taken to imply congestion, which triggers a congestion-control mechanism.
  - Finally, note that there is nothing about the Jacobson/Karels timeout computation that is specific to TCP. It could be used by any end-to-end protocol.
  - **The main problem with the original computation is that it does not take the variance of the sample RTTs into account. Intuitively, if the variation among samples is small, then the EstimatedRTT can be better trusted and there is no reason for multiplying this estimate by 2 to compute the timeout.**
  - **On the other hand, a large variance in the samples suggests that the timeout value should not be too tightly coupled to the EstimatedRTT.**
- In the new approach, the sender measures a new SampleRTT as before. It then folds this new sample into the timeout calculation as follows:

$$\text{Difference} = \text{SampleRTT} - \text{EstimatedRTT}$$

$$\text{EstimatedRTT} = \text{EstimatedRTT} + (\delta \times \text{Difference})$$

$$\text{Deviation} = \text{Deviation} + \delta(|\text{Difference}| - \text{Deviation})$$

- where  $\delta$  is a fraction between 0 and 1. That is, we calculate both the mean RTT and the variation in that mean.
- TCP then computes the timeout value as a function of both Estimated- RTT and Deviation as follows:

$$\text{TimeOut} = \mu \times \text{EstimatedRTT} + \phi \times \text{Deviation}$$

- where based on experience,  $\mu$  is typically set to 1 and  $\phi$  is set to 4.
- Thus, when the variance is small, TimeOut is close to EstimatedRTT; a large variance causes the Deviation term to dominate the calculation.

**9. Explain in detail about TCP congestion control mechanisms OR Brief about approaches used for TCP congestion control (NOV 2013, 2014, 2015, 2016,2017) OR With TCPs slow start and AIMD for congestion control,show how the window size will vary for a transmission where every 5<sup>TH</sup> Packet is lost.Assume an advertised window size of 50 MSS (Nov/Dec 2020).(April/may 2023),(April/may 24),(Nov/Dec 2023)**

#### Synopsis:

- **Introduction**
- **TCP Congestion Control**
- **Factors of congestion**
- **Congestion Window**
- **Congestion Policy**
  - **Slow start (Exponential Increase )**
  - **Additive Increase / Multiplicative Decrease**
  - **Fast Retransmit and Fast Recovery**

#### Introduction:

- 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 that can either prevent congestion before it happens or remove congestion, after it has happened.
- There are two categories of congestion control
  - **Open-loop congestion control (prevention):** are applied to prevent congestion before it happens. In this, congestion control is handled by either the source or the destination.

- **Closed-loop congestion control (removal):** try to remove congestion after it happens.

## TCP CONGESTION CONTROL

- Too many sources sending too much data too fast for network to handle. TCP uses congestion control to avoid congestion or remove congestion in the network.

### Factors of congestion:

- Two senders, two receivers
- One router, infinite buffers
- No retransmission
- One router, finite buffers, reliable data transfer
- Sender retransmission of lost packet

### Congestion Window

- The sender's window size is determined by the receiver and also by congestion in the network. The sender has two pieces of information:
  - i. The receiver – advertised window size (rwnd).
  - ii. The congestion window size (cwnd).
- The actual size of the window is the minimize of these two
   
Max window = min (Congestion window, advertised window)
   
Effective window = Max window – (LastByteSend – LastByteAcked)
   
LastByteSend – LastByteAcked <= CongWin

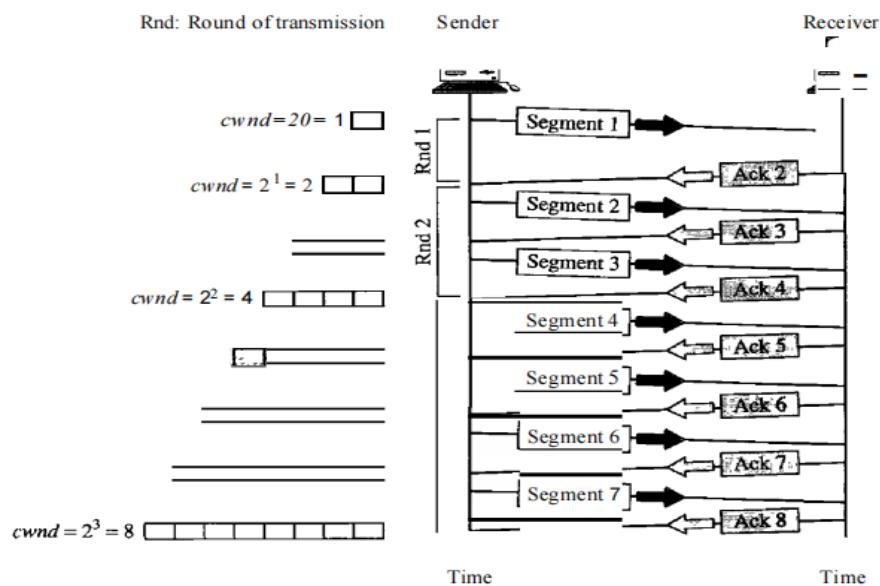
### Congestion Policy:

- TCP handles congestion is based on three phases
  - i. Slow start (Exponential Increase )
  - ii. Additive Increase / Multiplicative Decrease
  - iii. Fast Retransmit and Fast Recovery

#### i) Slow Start

- In this, the sender starts with a very slow rate of transmission but increases the rate rapidly to reach a threshold. (Refer fig 2.29)
- Slow start adds another window to the sender's TCP: the congestion window, called "cwnd". When a new connection is established with a host on another network, the congestion window is initialized to one segment.
- Each time an ACK is received, the congestion window is increased by one segment.

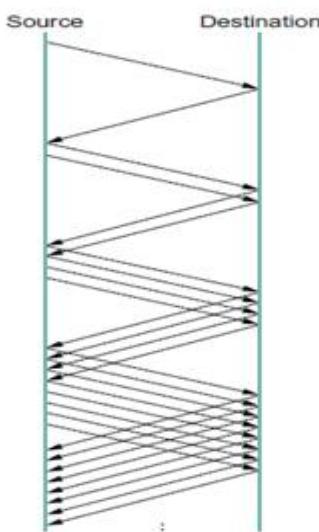
- The sender can transmit up to the minimum of the congestion window and the advertised window.
- The congestion window is flow control imposed by the sender, while the advertised window is flow control imposed by the receiver.
- The former is based on the sender's assessment of perceived network congestion; the latter is related to the amount of available buffer space at the receiver for this connection.
- The sender starts by transmitting one segment and waiting for its ACK. When that ACK is received, the congestion window is incremented from one to two, and two segments can be sent.
- When each of those two segments is acknowledged, the congestion window is increased to four.
- This provides an exponential growth, although it is not exactly exponential because the receiver may delay its ACKs, typically sending one ACK for every two segments that it receives.
- At some point the capacity of the internet can be reached, and an intermediate router will start discarding packets.
- This tells the sender that its congestion window has gotten too large.



**Fig 2.29 – Slow start**

- Early implementations performed slow start only if the other end was on a different network. Current implementations always perform slow start.
  - The source starts with cwnd = 1.
  - Every time an ACK arrives, cwnd is incremented.

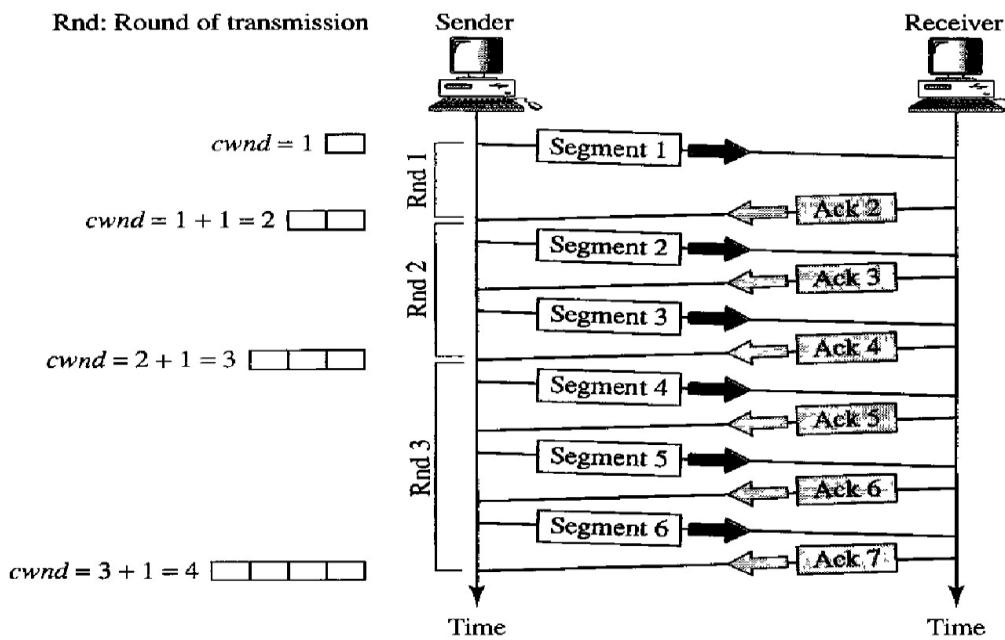
- Two slow start situations:
  - At the very beginning of a connection {**cold start**}.
  - When the connection goes dead waiting for a timeout to occur (i.e, the advertised window goes to zero!)
- However, in the second case the source has more information. The current value of cwnd can be saved as a **congestion threshold**.
- This is also known as the “slow start threshold” **ssthresh**.
- When the size of window in bytes reaches this threshold, slow start stops and the next phase starts. (Refer fig 2.30).



**Fig 2.30 – Packets in transit during slow start**

### ii) Additive Increase (Congestion avoidance) / Multiplicative Decrease

- To avoid congestion before it happens, one must slow down the exponential growth.
- When the size of the congestion window reaches the slow start threshold, the slow start phase steps and the additive phase begins.
- In this, each time the whole window of segments is acknowledged, the size of the congestion window is increased by 1. (Refer fig 2.31).

*Congestion avoidance, additive increase***Fig 2.31 – Additive Increase**

- After the sender has received acknowledgements for a complete window size of segments, the size of the congestion window increases additively until congestion is detected.
- The congestion window is incremented as follows each time an ACK arrives:

**Increment = MSS X (MSS / congestion window)**

**Congestion Window += Increment**

**Where MSS – Message Segment Size.**

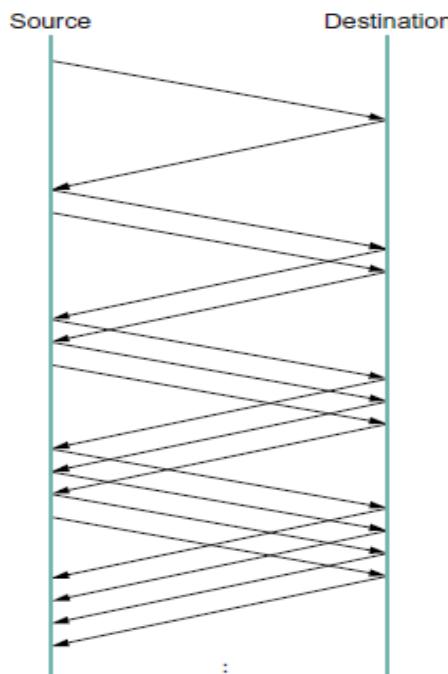
**Multiplicative Decrease:**

- If congestion occurs, the congestion window size must be decreased.
- Retransmission can occur in one of two cases, when a timer times out (or) when three ACKS are received.
- In both cases, the size of the threshold is dropped to one-half, a multiplicative decrease.

**TCP implementations have two reactions:**

- If a time-out occurs, there is a stronger possibility of congestion, a segment has probably been dropped in the network, and there is no news about the sent segments. In this, TCP reacts the following:
  - It sets the value of the threshold to one-half of the current window size.
  - It sets cwnd to the size of one segment.

- c. It starts the slow-start phase again.
2. If three ACK's are received, there is a weaker possibility of congestion, a segment may have been dropped, but some segments after that may have arrived safely since three ACKs are received. **This is called fast transmission and fast recovery.**
- o In this, TCP reacts the following: (Refer fig 2.32).
    - a) It sets the value of the threshold to one-half of the current window size.
    - b) It sets cwnd to the value of the threshold.
    - c) It starts the congestion avoidance phase.

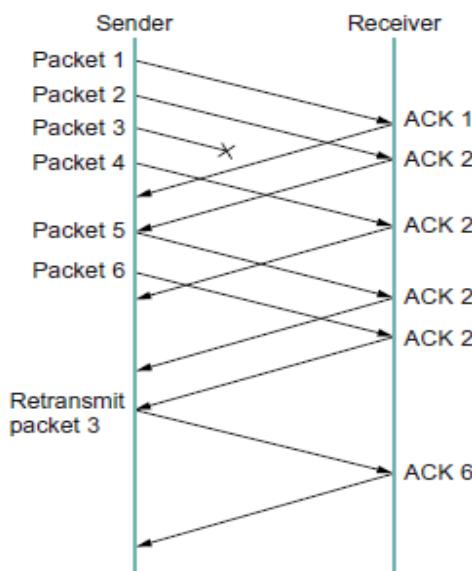


**Fig 2.32 – Packets in transit during additive increase with one packet being added each RTT**

### iii)Fast Retransmit & Fast Recovery

- Every time a data packet arrives at the receiving side, the receiver responds with an acknowledgement.
- When a packet arrives out of order, TCP resends the same acknowledgement it sent the last time.
- This second transmission of the same acknowledgement is called a **duplicate ACK**.
  - When the sending side sees a duplicate ACK, it knows that the other side must have received a packet out of order.

- The sender waits until it sees some no. of duplicate ACK's and then retransmit the missing packet.
- TCP waits until it has seen three duplicate ACK's before retransmitting the packet.
- In this diagram, the destination receives packets 1 & 2, but packet 3 is lost in the network.
- Thus the destination will send a duplicate ACK for packet 2 when packet 4 arrives, again when packet 5 arrives & so on.
- When the sender sees the third duplicate ACK for packet 2, the receiver had gotten packet 6, it retransmits packet 3.
- When the retransmitted copy of packet 3 arrives at the destination, the receiver then sends a cumulative ACK for everything up to and including packet 6 back to the sender. (Refer fig 2.33)



**Fig 2.33 – Fast retransmit based on duplicate ACKs**

### Fast Recovery

- After fast retransmit sends what appears to be the missing segment, congestion avoidance, but not slow start is performed.
- This is the fast recovery algorithm.
- It is an improvement that allows high throughput under moderate congestion, especially for large windows.
- The reason for not performing slow start in this case is that the receipt of the duplicate ACKs tells TCP more than just a packet has been lost.

- Since the receiver can only generate the duplicate ACK when another segment is received, that segment has left the network and is in the receiver's buffer.
  - That is, there is still data flowing between the two ends, and TCP does not want to reduce the flow abruptly by going into slow start.
  - The fast retransmit and fast recovery algorithms are usually implemented together as follows.
1. When the third duplicate ACK in a row is received, set ssthresh to one-half the current congestion window, cwnd, but no less than two segments. Retransmit the missing segment. Set cwnd to ssthresh plus 3 times the segment size. This inflates the congestion window by the number of segments that have left the network and which the other end has cached.
  2. Each time another duplicate ACK arrives, increment cwnd by the segment size. This inflates the congestion window for the additional segment that has left the network. Transmit a packet, if allowed by the new value of cwnd.
  3. When the next ACK arrives that acknowledges new data, set cwnd to ssthresh (the value set in step 1). This ACK should be the acknowledgment of the retransmission from step 1, one round-trip time after the retransmission. Additionally, this ACK should acknowledge all the intermediate segments sent between the lost packet and the receipt of the first duplicate ACK. This step is congestion avoidance, since TCP is down to one-half the rate it was at when the packet was lost.
  - When fast retransmit detects three duplicate ACKs, start the recovery process from congestion avoidance region and use ACKs in the pipe to pace the sending of packets.

**10. Write a detailed note on congestion avoidance mechanism used in TCP. NOV 2017 Or Explain congestion avoidance using random early detection in transport layer with example APR 2017,(Nov/Dec 2023)**

**Synopsis:**

- DEC bit
  - How it is functioning?
  - Random Early Detection (RED)
  - Source-Based Congestion Avoidance

**1. DEC Bit, 2. RED & 3. Source based Congestion Avoidance:****DEC bit**

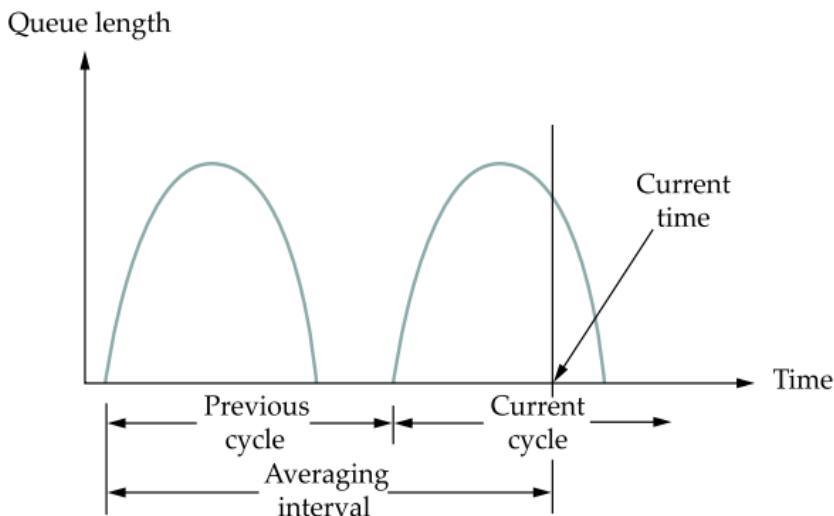
It is a first mechanism

- The idea here is to more evenly split the responsibility for congestion control between the routers and the end nodes.
- **Each router monitors the load it is experiencing and explicitly notifies the end nodes when congestion is about to occur.**
- This notification is implemented by setting a **binary congestion bit** in the packets that flow through the router: hence the name DECbit.
- The destination host then copies this congestion bit into the ACK it sends back to the source.
- Finally, the source adjusts its sending rate so as to avoid congestion.

**How it is functioning?**

- A single congestion bit is added to the packet header. A router sets this bit in a packet if its average queue length is greater than or equal to 1 at the time the packet arrives.
- This average queue length is measured over a time interval that distance the last burst + idle cycle, plus the current busy cycle. (The router is busy when it is transmitting and idles when it is not).
- The above figure shows the queue length at a router as a function of time. Essentially, the router calculates the area under the curve and divides this value by the time interval to compute the average queue length

If less than 50% of the packets had the bit set, then the source increases its congestion window by one packet. If 50% or more of the last window's worth of packets had the congestion bit set, the source decreases its congestion window to 0.875 times the previous value. (Refer fig 2.34)



**Fig 2.34 – Computing average queue length at a router**

### Random Early Detection (RED)

- A second mechanism, called random early detection (RED), is similar to the DECbit scheme in that each router is programmed to monitor its own queue length, and when it detects that congestion is imminent (forthcoming), to notify the source to adjust its congestion window.
- The first is that rather than explicitly sending a congestion notification message to the source, RED is most commonly implemented such that it implicitly notifies the source of congestion by dropping one of its packets.
- The source is, effectively notified by the subsequent timeout or duplicates ACK. In case you haven't already guessed, RED is designed to be used in conjunction with TCP, which currently detects congestion by means of timeouts.
- As the "early" part of the RED acronym suggests, the gateway drops the packet earlier than it would have to, so as to notify the source that it should decrease its congestion window sooner than it would normally have.
- In other words, the router drops a few packets before it has exhausted its buffer space completely, so as to cause the source to slow down, with the hope that this will mean it does not have to drop lots of packets later on.
- Note that RED could easily be adapted to work with an explicit feedback scheme simply by marking a packet instead of dropping it, as discussed in the sidebar on Explicit Congestion Notification.

### Source-Based Congestion Avoidance

- A strategy for detecting the initial stages of congestion – before losses occur – from the end hosts.
- The general idea of these techniques is to watch for some sign from the network that some router's queue is building up and that congestion will happen soon if nothing is done about it.
- A **first Scheme** the congestion window normally increases as in TCP, but every two round-trip delays the algorithm checks to see if the current RTT is greater than the average of the minimum and maximum RTT's seen so far. If it is, then the algorithm decreases the congestion window by one-eighth.
- A **second algorithm** is the decision as to whether or not to change the current window size is based on changes to both the RTT and the window size. The window is adjusted once every two round-trip delays based on the product

$$(CurrentWindow - OldWindow) \times (CurrentRTT - OldRTT)$$

If the result is positive, the source decreases the window size by one-eighth; if the result is negative or 0, the source increases the window by one maximum packet size.

- A **third scheme**, Every RTT, it increases the window size by one packet and compares the throughput achieved to the throughput when the window was one packet smaller. If the difference is less than one-half the throughput achieved when only one packet was in transit. If the difference is greater than the algorithm decreases the window by one packet. This scheme calculates the throughput by dividing the number of bytes outstanding in the network by the RTT.
- A **fourth mechanism**, it looks at changes in the throughput rate, or more specifically, changes in the sending rate.
- It compares the measured throughput rate with an expected throughput rate. The algorithm, which is called **TCP Vegas**.
- TCP Vegas uses this idea to measure and control the amount of extra data this connection has in transit, where by "extra data" we mean that the source would not have transmitted had it been trying to match exactly the available bandwidth of the network.

- The goal of TCP Vegas is to maintain the “right” amount of extra data in the network.
- Obviously, if a source is sending too much extra data, it will cause long delays and possibly lead to congestion. Less obviously, if a connection is sending too little extra data, it cannot respond rapidly enough to transient increases in the available network bandwidth.
  - ✓ TCP Vegas sets BaseRTT to the minimum of all measured round-trip times; it is commonly the RTT of the first packet sent by the connection, before the router queues increase due to traffic generated by this flow. If we assume that we are not overflowing the connection, then the expected throughput is given by

$$\text{Expected Rate} = \text{Congestion Window} / \text{BaseRTT}$$

Where CongestinWindow is the TCP congestion window, which we assume (for the purpose of this discussion) to be equal to the number of bytes in transit.

- ✓ Second TCP Vegas calculates the current sending rate, ActualRate. This is done by recording the sending time for a distinguished packet, recording how many bytes are transmitted between the time that packet is sent and when its acknowledgment is received, computing the sample RTT for the distinguished packet when its acknowledgment arrives, and dividing the number of bytes transmitted by the sample RTT. This calculation is done once per round-trip time.
- ✓ Third, TCP Vegas compares ActualRate to ExpectedRate and adjusts the window accordingly. We let Diff = ExpectedRate - ActualRate. Note that Diff is positive or 0 by definition, since ActualRate > ExpectedRate implies that we need to change BaseRTT to the latest sampled RTT.
- We also define two thresholds,  $\alpha < \beta$ , roughly corresponding to having too little and too much extra data in the network, respectively.
- When  $\text{Diff} < \alpha$ , TCP Vegas increases the congestion window linearly during the next RTT, and when  $\text{Diff} > \beta$ , TCP Vegas decreases the congestion window linearly during the next RTT.
- TCP Vegas leaves the congestion window unchanged when  $\alpha < \text{Diff} < \beta$ .

## 11. Explain SCTP (Stream Control Transmission Protocol) in detail

(Nov/Dec 2020).

### Synopsis:

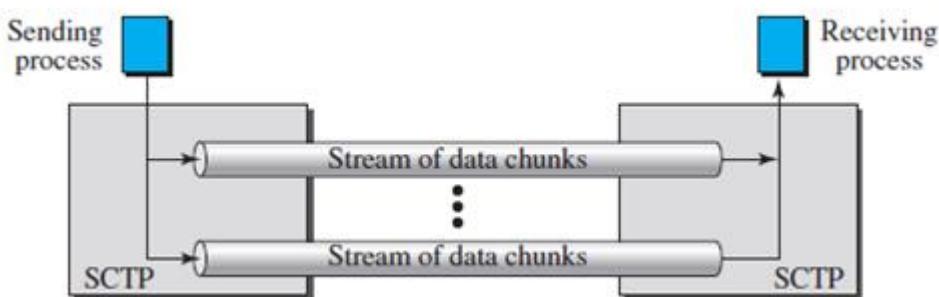
- **Definition**
- **SCTP Services**
  - **Process-to-Process Communication**
  - **Multiple Streams**
- **SCTP Features**
- **SCTP Packet Format**
- **Types of Chunks**
- **An SCTP Association**

### Definition:

**Stream Control Transmission Protocol (SCTP)** is a new transport-layer protocol designed to combine some features of UDP and TCP in an effort to create a better protocol for multimedia communication.

### SCTP Services

- **Process-to-Process Communication**
- **Multiple Streams**
- SCTP allows **multi stream service** in each connection, which is called **association** in SCTP terminology. If one of the streams is blocked, the other streams can still deliver their data. (Refer fig 2.35).

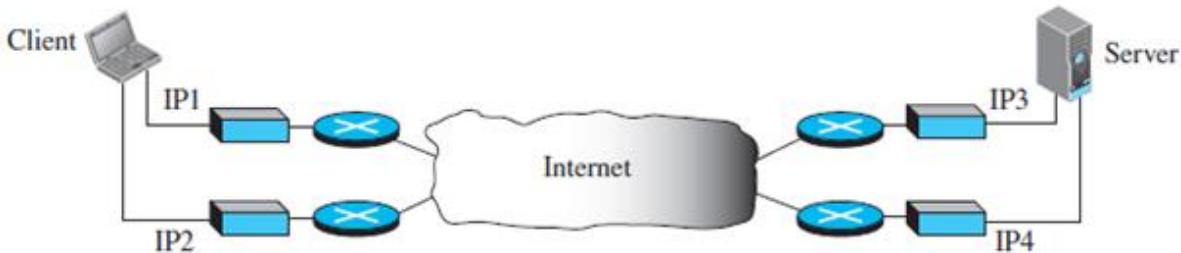


**Fig 2.35 – Multiple-stream concept**

### • Multihoming

- The sending and receiving host can define multiple IP addresses in each end for an association. In this fault-tolerant approach, when one path fails, another interface can be used for data delivery without interruption.

- This fault-tolerant feature is very helpful when we are sending and receiving a real-time payload such as Internet telephony. (Refer fig 2.36).



**Fig 2.36 – Multihoming concept**

- **Full-Duplex Communication**
- **Connection-Oriented Service**
- **Reliable Service**

### SCTP Features

#### Transmission Sequence Number (TSN)

- The unit of data in SCTP is a data chunk, which may or may not have a one-to-one relationship with the message coming from the process because of fragmentation.
- Data transfer in SCTP is controlled by numbering the data chunks.
- SCTP uses a **transmission sequence number (TSN)** to number the data chunks.
- In other words, the TSN in SCTP plays a role analogous to the sequence number in TCP.

#### Stream Identifier (SI)

- In SCTP, there may be several streams in each association. Each stream in SCTP needs to be identified using a **stream identifier (SI)**.
- Each data chunk must carry the SI in its header so that when it arrives at the destination, it can be properly placed in its stream.
- The SI is a 16-bit number starting from 0.

#### Stream Sequence Number (SSN)

- When a data chunk arrives at the destination SCTP, it is delivered to the appropriate stream and in the proper order.
- This means that, in addition to an SI, SCTP defines each data chunk in each stream with a **stream sequence number (SSN)**.

**Acknowledgment Number**

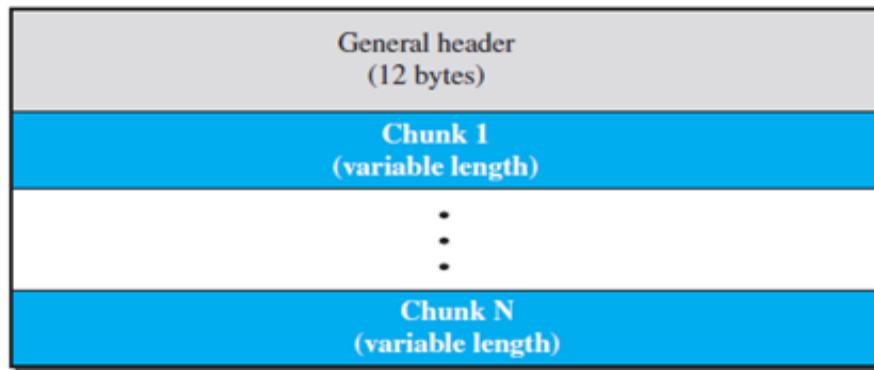
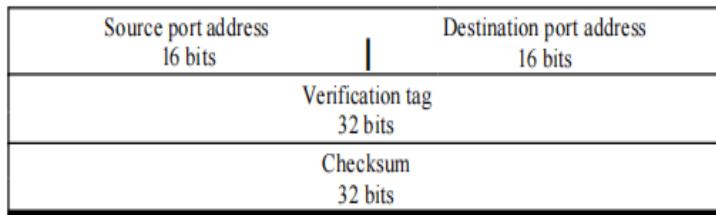
- TCP acknowledgment numbers are byte-oriented and refer to the sequence numbers.
- SCTP acknowledgment numbers are chunk-oriented.
- They refer to the TSN.
- A second difference between TCP and SCTP acknowledgments is the control information

**SCTP Packet Format**

- An SCTP packet has a mandatory general header and a set of blocks called **chunks**.
- There are two types of chunks: control chunks and data chunks.
- A control chunk controls and maintains the association; a data chunk carries user data.
- In a packet, the control chunks come before the data chunks. Figure 2.37 shows the general format of an SCTP packet.

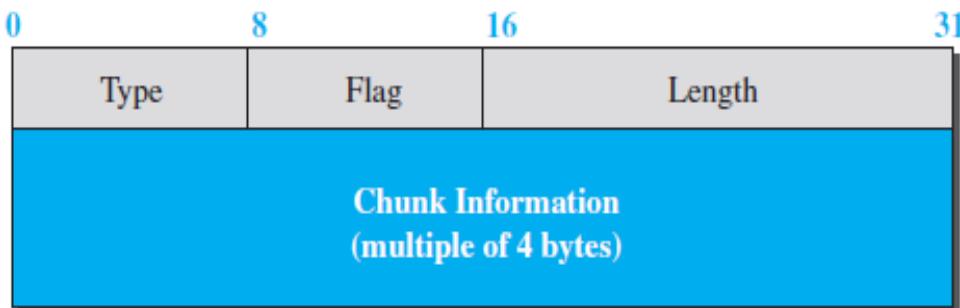
**General Header**

- The *general header* (packet header) defines the end points of each association to which the packet belongs, guarantees that the packet belongs to a particular association, and preserves the integrity of the contents of the packet including the header itself.
- The format of the general header is shown in Figure 2.38.
- There are four fields in the general header.
- The source and destination port numbers are the same as in UDP or TCP.
- The verification tag is a 32-bit field that matches a packet to an association.
- This prevents a packet from a previous association from being mistaken as a packet in this association.
- It serves as an identifier for the association; it is repeated in every packet during the association.
- The next field is a checksum. However, the size of the checksum is increased from 16 bits (in UDP, TCP, and IP) to 32 bits in SCTP to allow the use of the CRC-32 checksum.

**Fig 2.37 – SCTP packet format****Fig 2.38 – General header**

### Chunks

- Control information or user data are carried in chunks.
- Chunks have a common layout. The first three fields are common to all chunks; the information field depends on the type of chunk (Refer fig 2.39)

**Fig 2.39 – Common layout of a chunk**

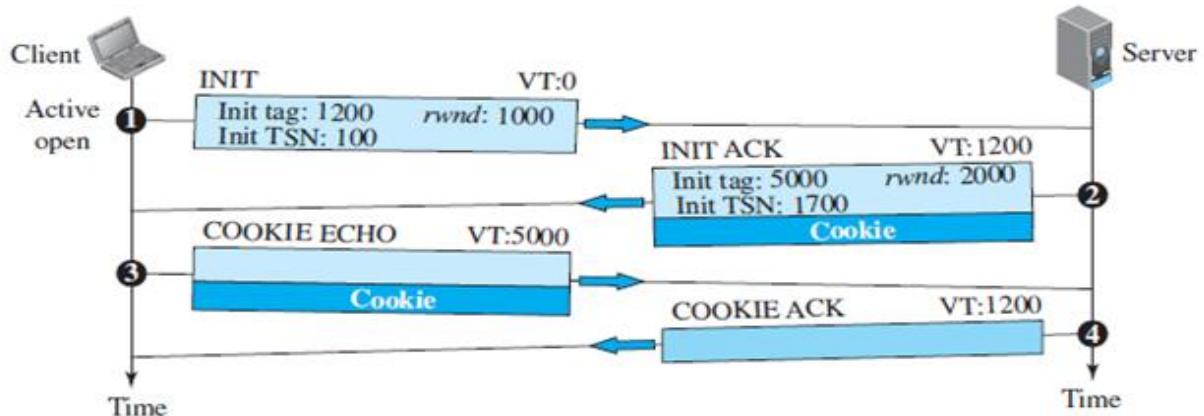
### Types of Chunks

SCTP defines several types of chunks

Type	Chunk	Description
0	DATA	User data
1	INIT	Sets up an association
2	INIT ACK	Acknowledges INIT chunk
3	SACK	Selective acknowledgment
4	HEARTBEAT	Probes the peer for liveness
5	HEARTBEAT ACK	Acknowledges HEARTBEAT chunk
6	ABORT	Aborts an association
7	SHUTDOWN	Terminates an association
8	SHUTDOWN ACK	Acknowledges SHUTDOWN chunk
9	ERROR	Reports errors without shutting down
10	COOKIE ECHO	Third packet in association establishment
11	COOKIE ACK	Acknowledges COOKIE ECHO chunk
14	SHUTDOWN COMPLETE	Third packet in association termination
192	FORWARD TSN	For adjusting cumulating TSN

**Table 2.4 - Chunks****An SCTP Association**

- SCTP, like TCP, is a connection-oriented protocol. However, a connection in SCTP is called an *association* to emphasize multihoming (Refer fig 2.40).
- **Association Establishment**
- **Data Transfer**
  - Multihoming Data Transfer
  - Multistream Delivery
  - Fragmentation
- **Association Termination** (Refer fig 2.41)

**Fig 2.40 – Four-way handshaking**

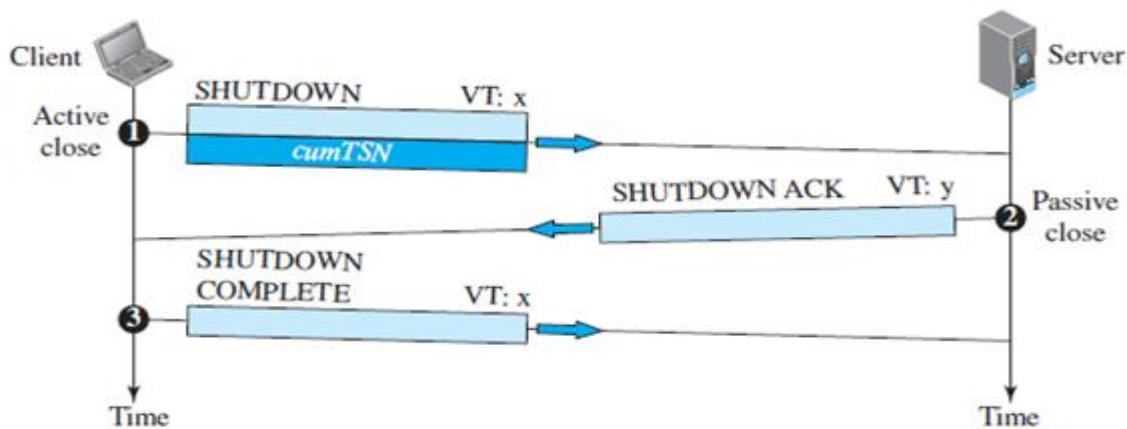


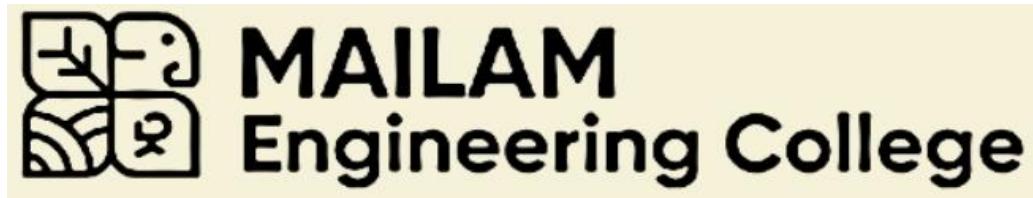
Fig 2.41 – Association termination

**12. Compare and Contrast of UDP and TCP protocols. Explain it briefly (April/May 2024)**

Basis	Transmission Protocol (TCP)	Control	User Datagram Protocol (UDP)
Type of Service	<b>TCP</b> is a connection-oriented protocol. Connection orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data.	<b>UDP</b> is the Datagram-oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, or terminating a connection. UDP is efficient for broadcast and multicast types of network transmission.	
Reliability	TCP is reliable as it guarantees the delivery of data to the destination router.	The delivery of data to the destination cannot be guaranteed in UDP.	
Error checking mechanism	TCP provides extensive error-checking mechanisms. It is because it provides flow control and acknowledgment of data.	UDP has only the basic error-checking mechanism using checksums.	

<b>Basis</b>	<b>Transmission Protocol (TCP)</b>	<b>Control</b>	<b>User Datagram Protocol (UDP)</b>
<b>Acknowledgment</b>	An acknowledgment segment is present.		No acknowledgment segment.
<b>Sequence</b>	Sequencing of data is a feature of Transmission Control Protocol (TCP). This means that packets arrive in order at the receiver.		There is no sequencing of data in UDP. If the order is required, it has to be managed by the application layer.
<b>Speed</b>	TCP is comparatively slower than UDP.		UDP is faster, simpler, and more efficient than TCP.
<b>Retransmission</b>	Retransmission of lost packets is possible in TCP, but not in UDP.		There is no retransmission of lost packets in the User Datagram Protocol (UDP).
<b>Header Length</b>	TCP has a (20-60) bytes variable length header.		UDP has an 8 bytes fixed-length header.
<b>Weight</b>	TCP is heavy-weight.		UDP is lightweight.
<b>Handshaking Techniques</b>	Uses handshakes such as SYN, ACK, SYN-ACK		It's a connectionless protocol i.e. No handshake
<b>Broadcasting</b>	TCP doesn't support Broadcasting.		UDP supports Broadcasting.
<b>Protocols</b>	TCP is used by HTTP, HTTPS, FTP, SMTP and Telnet .		UDP is used by DNS, DHCP, TFTP, SNMP, RIP, and VoIP .
<b>Stream Type</b>	The TCP connection is a byte		UDP connection is a

	<b>Transmission Protocol (TCP)</b>	<b>Control</b>	<b>User Datagram Protocol (UDP)</b>
<b>Basis</b>			
	stream.		message stream.
<b>Overhead</b>	Low but higher than UDP.		Very low.
<b>Applications</b>	This protocol is primarily utilized in situations when a safe and trustworthy communication procedure is necessary, such as in email, on the web surfing, and in military services.		This protocol is used in situations where quick communication is necessary but where dependability is not a concern, such as VoIP, game streaming, video, and music streaming, etc



(Approved by AICTE, New Delhi, Affiliated to Anna University Chennai, Accredited by NBA, TCS & NAAC - 'A' Grade)

**DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND DATA SCIENCE**

**II YEAR / IV SEM**

**CS3591 – COMPUTER NETWORKS**

**UNIT III – NETWORK LAYER**

**SYLLABUS:**

Switching: Packet Switching - Internet protocol - IPV4 – IP Addressing – Subnetting - IPV6, ARP, RARP, ICMP, DHCP

**PART A**

**1. List the various services provided in the Network Layer.**

- Packetizing
- Routing and Forwarding
- Other Services
  - Error Control
  - Flow Control
  - Congestion Control
  - Quality of Service
  - Security

**2. Define packetizing.**

- **Packetizing:** encapsulating the payload (data received from upper layer) in a network-layer packet at the source and decapsulating the payload from the network-layer packet at the destination.

**3. Define Routing and Forwarding.****Routing**

- The network layer is responsible for routing the packet from its source to the destination.

**Forwarding**

- Forwarding can be defined as the action applied by each router when a packet arrives at one of its interfaces.

**4. Define packet switched network and list the different approaches to route the packet.****Packet Switched Network:**

- Packet switching is used at the network layer because the unit of data at this layer is a packet.
- At the network layer, a message from the upper layer is divided into manageable packets and each packet is sent through the network.
- A packet-switched network can use two different approaches to route the packets:
  - The **datagram approach** - Connectionless Service
  - The **virtual circuit approach** - Connection-Oriented Service.

**5. Narrate how the performance of a network can be measured?**

- The performance of a network can be measured in terms of
  - delay,
  - transmission delay,
  - propagation delay,
  - processing delay,
  - queuing delay.
  - throughput,
  - packet loss.
  - Congestion Control

**6. Define Transmission delay.**

- A sender needs to put the bits in a packet one by one.
- The transmission delay is longer for a longer packet and shorter if the sender can transmit faster.
- In other words, the transmission delay is

$$\text{Delay}_{\text{tr}} = (\text{Packet length}) / (\text{Transmission rate}).$$

**7. Define Propagation Delay.**

- Propagation delay is the time it takes for a bit to travel from point A to point B in the transmission media.

$$\text{Delay}_{\text{pg}} = (\text{Distance}) / (\text{Propagation speed}).$$

**8. Define Processing Delay.**

- The processing delay is the time required for a router or a destination host to receive a packet from its input port, remove the header, perform an error detection procedure, and deliver the packet to the output port (in the case of a router) or deliver the packet to the upper-layer protocol (in the case of the destination host).

$$\text{Delay}_{\text{pr}} = \text{Time required to process a packet in a router or a destination host}$$

**9. Define Queuing Delay.**

- The queuing delay for a packet in a router is measured as the time a packet waits in the input queue and output queue of a router.

$$\text{Delay}_{\text{qu}} = \text{The time a packet waits in input and output queues in a router}$$

**10. Define Throughput.**

- Throughput at any point in a network is defined as the number of bits passing through the point in a second, which is actually the transmission rate of data at that point.
- In a path from source to destination, a packet may pass through several links (networks), each with a different transmission rate.

$$\text{Throughput} = \min \{\text{TR}_1, \text{TR}_2, \dots, \text{TR}_n\}.$$

**11. Define Congestion Control and mention its types.**

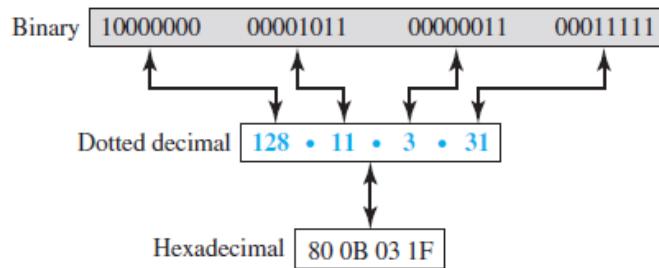
- Congestion control is a mechanism for improving performance.
- Two broad categories:
  - open-loop congestion control (prevention)
  - closed-loop congestion control (removal).

**12. Define IPv4 Address and list the various types of notations.**

- An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a host or a router to the Internet.
- IPv4 addresses are unique. If a device has two connections to the Internet, via two networks, it has two IPv4 addresses.

**Notation**

- There are three common notations to show an IPv4 address: binary notation (base 2), dotted-decimal notation (base 256), and hexadecimal notation (base 16).

**13. Define and Differentiate Classful and Classless Addressing.****Classful Addressing.**

- An IPv4 address was designed with a fixed-length prefix. The whole address space was divided into five classes (class A, B, C, D, and E). This scheme is referred to as classful addressing.

**Classless Addressing**

- In addressing, the whole address space is divided into variable length classless blocks.
- The prefix in an address defines the block (network); the suffix defines the node (device).
- A prefix length ranges from 0 to 32.

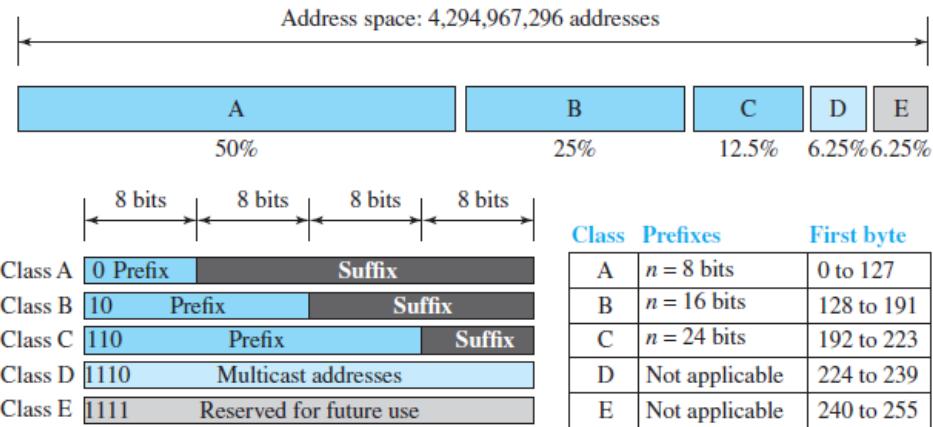
**Difference between Classless Addressing and Classful Addressing**

<b>Classful Addressing</b>	<b>Classless Addressing</b>
An IP Address allocation method that allocates IP addresses according to five major classes.	An IP Address allocation method that is designed to replace classful addressing to minimize the rapid exhaustion of IP addresses.
Less practical and useful.	More practical and useful.
Network ID and host ID changes depending on the classes.	There is no boundary on Network ID and host ID
Addresses have three parts: network, subnet, and host.	Addresses have two parts: subnet or prefix, and host.
IP forwarding process is restricted in how it uses the default route	IP forwarding process has no restrictions on using the default route
Routing protocol does not advertise masks nor support VLSM; RIP-1 and IGRP	Routing protocol does advertise masks and support VLSM; RIP-2, EIGRP, OSPF.

**14. Define Address Masking.**

- The address mask is a 32-bit number in which the n leftmost bits are set to 1s and the rest of the bits (32 - n) are set to 0s.
- To extract the information in a block, using the three bit-wise operations NOT, AND, and OR.
  1. The number of addresses in the block  $N = \text{NOT}(\text{mask}) + 1$ .
  2. The first address in the block = (Any address in the block) AND (mask).
  3. The last address in the block = (Any address in the block) OR [(NOT (mask))].

**15. Specify the various types of Classes and its range in Classful Addressing.**



**16. A classless address is given as 167.199.170.82/27. Find the number of addresses, First address and last address of the block.**

**Solution:**

- The **number of addresses** in the network is  $2^{32} - n = 2^5 = 32$  addresses.
- The **first address** can be found by keeping the first 27 bits and changing the rest of the bits to 0s.

**Address:**

167.199.170.82/**27** 10100111 11000111 10101010 01010010

**First address:**

167.199.170.64/**27** 10100111 11000111 10101010 010**00000**

- The **last address** can be found by keeping the first 27 bits and changing the rest of the bits to 1s.

**Address:**

167.199.170.82/**27** 10100111 11000111 10101010 01011111

**Last address:**

167.199.170.95/27 10100111 11000111 10101010 010**11111**

**17. An organization is granted a block of addresses with the beginning address 14.24.74.0/24. The organization needs to have 3 subblocks of addresses to use in its three subnets: one subblock of 10 addresses, one subblock of 60 addresses, and one subblock of 120 addresses. Design the subblocks.**

**Solution:**

- There are  $2^{32} - 2^4 = \mathbf{256 \text{ addresses}}$  in this block.
- The first address is **14.24.74.0/24**; the last address is **14.24.74.255/24**.

**Subblock with 120 addresses:**

- The number of addresses in the largest subblock, which requires 120 addresses, is not a power of 2. We allocate **128 addresses**.
- The subnet mask for this subnet can be found as  $n1 = 32 - \log_2 128 = \mathbf{25}$ . The first address in this block is **14.24.74.0/25**; the last address is **14.24.74.127/25**.

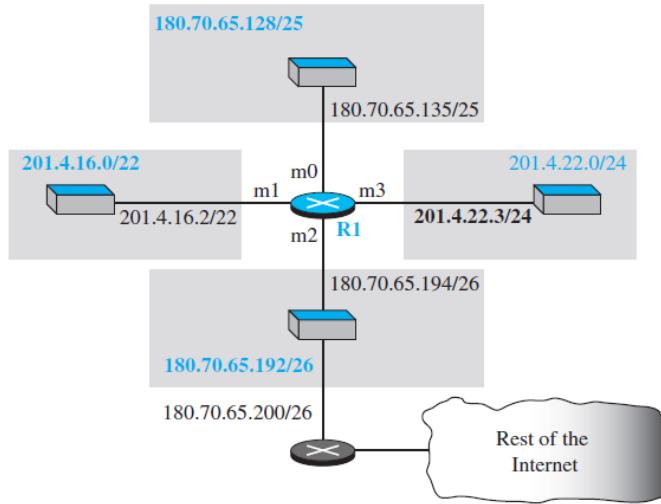
**Subblock with 60 addresses:**

- The number of addresses in the second largest subblock, which requires 60 addresses, is not a power of 2 either. We allocate **64 addresses**.
- The subnet mask for this subnet can be found as  $n2 = 32 - \log_2 64 = \mathbf{26}$ .
- The first address in this block is **14.24.74.128/26**; the last address is **14.24.74.191/26**.

**Subblock with 10 addresses:**

- The number of addresses in the smallest subblock, which requires 10 addresses, is not a power of 2 either. We allocate **16 addresses**.
- The subnet mask for this subnet can be found as  $n3 = 32 - \log_2 16 = \mathbf{28}$ .
- The first address in this block is **14.24.74.192/28**; the last address is **14.24.74.207/28**.
- If we add all addresses in the previous subblocks, the result is **208 addresses**. The first address in this range is **14.24.74.208**. The last address is **14.24.74.255**.

**18. Make a forwarding table for router R1 using the configuration in Figure**



**Solution:**

Network address/mask	Next hop	Interface
180.70.65.192/26	—	m2
180.70.65.128/25	—	m0
201.4.22.0/24	—	m3
201.4.16.0/22	—	m1
Default	180.70.65.200	m2

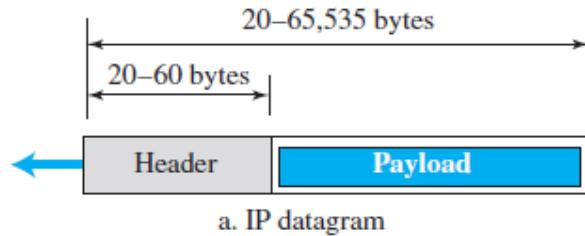
**19. How the IP packets are forwarded?**

**FORWARDING OF IP PACKETS**

- Forwarding Based on Destination Address
- Forwarding Based on Label

**20. Define Datagram.**

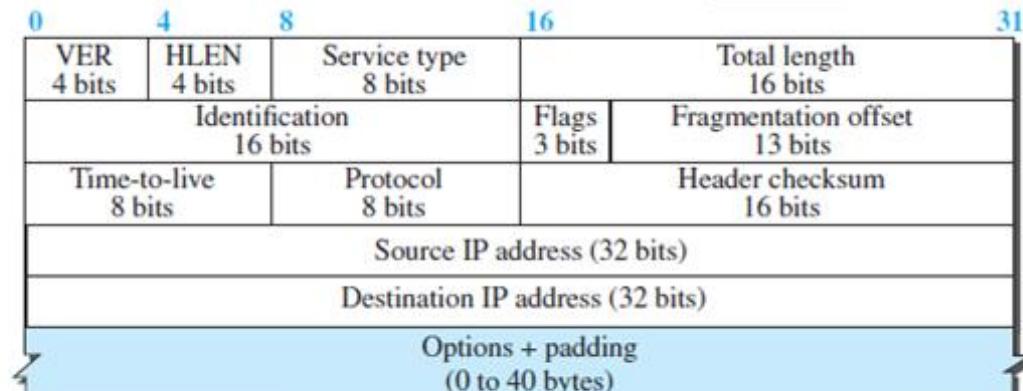
- Packets used by the IP are called datagrams.
- A datagram is a variable-length packet consisting of two parts: header and payload (data).
- The header is 20 to 60 bytes in length and contains information essential to routing and delivery.



a. IP datagram

**21. What is IPv4? Mention its IPv4 packet format.**

- The Internet Protocol version 4 (IPv4), is responsible for packetizing, forwarding, and delivery of a packet at the network layer.



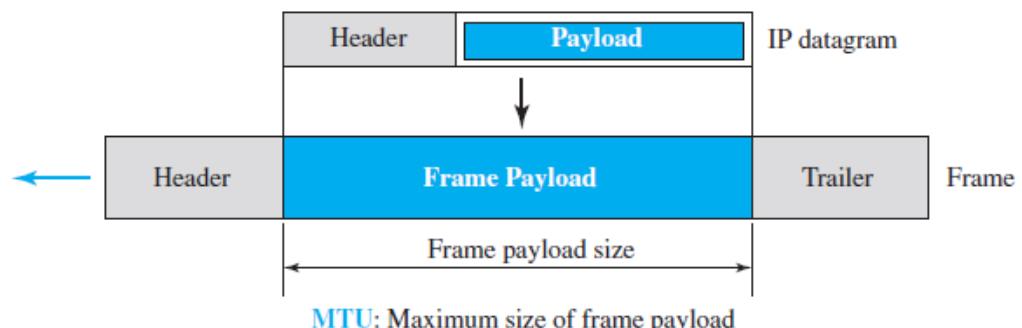
b. Header

**22. Define fragmentation and explain how it is performed.****➤ Fragmentation**

- The division of a packet into smaller units to accommodate a protocol's MTU.

**Maximum Transfer Unit (MTU)**

- The largest size data unit a specific network can handle.



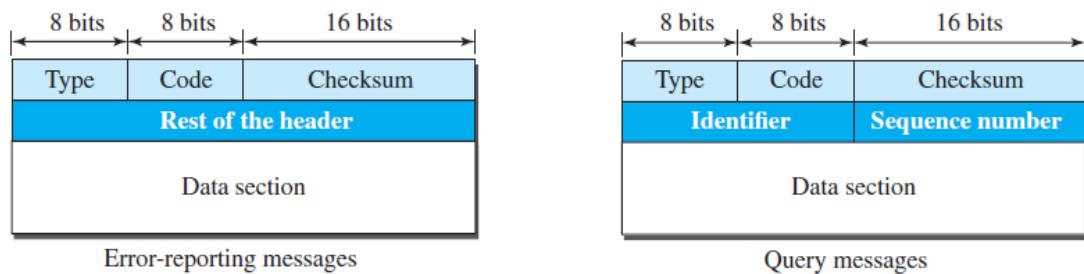
- When a datagram is fragmented, each fragment has its own header with most of the fields repeated, but some have been changed.
- A datagram may be fragmented several times before it reaches the final destination.

**23. Narrate the purpose of Internet Control Message Protocol version 4 (ICMPv4) message.**

- The Internet Control Message Protocol version 4 (ICMPv4) helps IPv4 to handle some errors that may occur in the network-layer delivery.
- ICMP is used to report some errors that may occur during the processing of the IP datagram. ICMP does not correct errors, it simply reports them.

**24. List the various ICMPv4 Error Messages.**

- ICMP messages are divided into two broad categories: error-reporting messages and query messages



**Type and code values**

**Error-reporting messages**

- 03: Destination unreachable (codes 0 to 15)
- 04: Source quench (only code 0)
- 05: Redirection (codes 0 to 3)
- 11: Time exceeded (codes 0 and 1)
- 12: Parameter problem (codes 0 and 1)

**Query messages**

- 08 and 00: Echo request and reply (only code 0)
- 13 and 14: Timestamp request and reply (only code 0)

**25. List and define the two debugging tools used in ICMPv4 messages. Or Define Ping and Traceroute.**

- Two debugging tools: ping and traceroute.

**Ping**

- Ping program is used to find if a host is alive and responding.
- The source host sends ICMP echo-request messages; the destination, if alive, responds with ICMP echo-reply messages.
- The ping program gets help from two query messages;

**Traceroute or Tracert**

- The traceroute program in UNIX or tracert in Windows can be used to trace the path of a packet from a source to the destination.
- It can find the IP addresses of all the routers that are visited along the path.
- The traceroute program gets help from two error-reporting messages: time-exceeded and destination-unreachable.

**26. An example of a checksum calculation for an IPv4 header without options. The header is divided into 16-bit sections. All the sections are added and the sum is complemented after wrapping the leftmost digit. The result is inserted in the checksum field.**

4	5	0	28		
49.153		0	0		
4	17	0			
10.12.14.5					
12.6.7.9					
4, 5, and 0	→	4	5	0	0
28	→	0	0	1	C
1	→	C	0	0	1
0 and 0	→	0	0	0	0
4 and 17	→	0	4	1	1
0	→	0	0	0	0
10.12	→	0	A	0	C
14.5	→	0	E	0	5
12.6	→	0	C	0	6
7.9	→	0	7	0	9
Sum	→	1	3	4	E
Wrapped sum	→	3	4	4	F
Checksum	→	C	B	B	0

Replaces 0

**27. List the security issues practically applicable to IP Datagrams.**

- There are three security issues that are particularly applicable to the IP protocol:
  - packet sniffing,
  - packet modification,
  - IP spoofing.

**Packet Sniffing**

- Packet sniffing is a passive attack, in which the attacker does not change the contents of the packet.
- This type of attack is very difficult to detect because the sender and the receiver may never know that the packet has been copied.

**Packet Modification**

- The attacker intercepts the packet, changes its contents, and sends the new packet to the receiver.
- The receiver believes that the packet is coming from the original sender.
- This type of attack can be detected using a data integrity mechanism.

**IP Spoofing**

- An attacker can masquerade as somebody else and create an IP packet that carries the source address of another computer.
- An attacker can send an IP packet to a bank pretending that it is coming from one of the customers.
- This type of attack can be prevented using an origin authentication mechanism

**28. How IP packets are protected from various security issues?****IPSec**

- The IP packets today can be protected from the security attacks using a protocol called IPSec (IP Security).

**IPSec provides the following four services:**

- Defining Algorithms and Keys.
- Packet Encryption.
- Data Integrity.
- Origin Authentication.

**29. Define Sub netting.**

- Sub netting provides an elegantly simple way to reduce the total number of network numbers that are assigned.
- The idea is to take a single IP network number and allocate the IP address with that network to several physical networks, which are now referred to as subnets.

**30. What is DHCP? (NOV/DEC 2012)**

- Dynamic Host Configuration Protocol (DHCP) is a protocol designed to provide information dynamically.
- It is a client-server program.
- DHCP is used to assign addresses to a host dynamically.
- Basically, DHCP server has two databases.
- The first database is addresses to IP addresses.

**31. What are the salient features of IPV6? (NOV/DEC 2020)**

- New Packet Format and Header
- Large Address Space
- State full and Stateless IPv6 address
- Multicast
- Integrated

**32. What are the different routing techniques available to manage routing table entries?**

1. Next hop routing.
2. Network specific routing.
3. Host specific routing.
4. Default routing.

**33. What is IPv6?**

- **Internet Protocol version 6 (IPv6)** is the latest revision of the **Internet Protocol (IP)**, the communications that provides an identification and location system for computers on networks and routes traffic across the Internet.
- IPv6 was developed by the **Internet Engineering Task Force (IETF)** to deal with the long-anticipated problem of **IPv4 address exhaustion**.

**34. Discuss Congestion avoidance in network layer.**

- Congestion occurs in a computer network when the resource demands exceed the capacity. Packets may be lost due to too much queuing in the network.

- During congestion, the network throughput may drop and the path delay may become very high.
- A congestion control scheme helps the network to recover from the congestion state.
- A congestion avoidance scheme allows a network to operate in the region of low delay and high throughput. Such schemes prevent a network from entering the congested state.
- Congestion avoidance is a prevention mechanism while congestion control is a recovery mechanism.

**35. What is the need of sub netting? (NOV/DEC 2013 & 2015).**

- When we divide a network into several subnets, we have three levels of hierarchy
  - The netid is the first level, defines the site.
  - The subnetid is the 2nd level, defines the physical subnetwork.
  - The hostid is the 3rd level defines the connection of the host to the subnetwork.

**36. What is a hostid and netid?**

- **Netid** – The portion of the IP address that identifies the network called the netid.
- **Hostid** – The portion of the IP address that identifies the host or router on the network is called the hostid.

**37. What is the difference between boundary level masking and non-boundary level masking?****• Boundary level Masking:**

If the masking is at the boundary level, the mask numbers are either 255 or 0, finding the subnetwork address is very easy.

**• Non Boundary level Masking**

If the masking is not at the boundary level, the mask numbers are not just 255 or 0, finding the subnetwork address involves using the bitwise AND operators.

**38. How does a router differ from a bridge?**

- Routers provide links between two separate but same type LANs and are most active at the network layer.
- Whereas bridges utilize addressing protocols and can affect the flow control of a single LAN; most active at the data link layer.

**39. Identify the class and default subnet mask of the IP address****217.65.10.7.**

It belongs to class C.

Default subnet mask – 255.255.255.192

**40. What is the time to live field in IP header?**

- Time to live field is counter used to limit packet lifetimes counts in second and default value is 255 sec.

**41. List the difference between IPv4 and IPv6 (Nov 2021)**

<b>IPv4</b>	<b>IPv6</b>
IPv4 has a 32-bit address length	IPv6 has a 128-bit address length
It Supports Manual and DHCP address configuration	It supports Auto and renumbering address configuration
In IPv4 end to end, connection integrity is Unachievable	In IPv6 end to end, connection integrity is Achievable

**42. Define the function of a Router. (Nov 2021)**

A router is a device that connects two or more packet-switched networks or subnetworks. It serves two primary functions: managing traffic between these networks by forwarding data packets to their intended IP addresses, and allowing multiple devices to use the same Internet connection.

**43. What is (Differ) ARP and RARP? (MAY/JUNE 2009).**

- ARP stands for Address Resolution Protocol. It is used to **convert IP address to Physical address.**
- RARP stands for Reverse Address Resolution Protocol. It is used to convert **Physical address into IP address.**

**44. What is the need for ARP? (NOV/DEC 2013) (Nov 2015).**

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network. For example, in IP Version 4, the most common level of IP in use today, an address is 32 bits long.

In an Ethernet local area network, however, addresses for attached devices are 48 bits long. (The physical machine address is also known as a Media Access Control or MAC address.) A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions.

**45. Define switching & list its types.****Switching**

- To make communication among multiple devices efficiently, a process used is called switching.
- A switched network consists of a series of interlinked nodes called switches.

**Type of switching**

- Circuit Switching
- Packet Switching
- Message Switching

**46. Write down any two differences between circuit switching and packet switching.**

(Nov/Dec 2020) (May 2017)

**Circuit switching**

- In circuit switching network dedicated channel has to be established before the call is made between users
- The channel is reserved between the users till the connection is active

**Packet switching**

- In packet switching network unlike CS network, it is not required to establish the connection initially
- The connection/channel is available to use by many users.

**47.Define Tunnelling?(April/may 2023)**

- Tunneling is a way to move packets from one network to another.
- Tunneling works via encapsulation
- wrapping a packet inside another packet.

**48.Difference between CSMA Collision Avoidance and Collision Detection?(April/may 2023)**

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) and Carrier Sense Multiple Access with Collision Detection (CSMA/CD) are two protocols used to manage data transmission in networks. While CSMA/CA is commonly used in wireless networks, CSMA/CD is used in wired networks.

<b>CSMA/CA</b>	<b>CSMA/CD</b>
CSMA / CA is effective before a collision.	CSMA / CD is effective after a collision.
CSMA / CA is commonly used in wireless networks.	CSMA / CD is used in wired networks.
CSMA/ CA minimizes the possibility of collision.	It only reduces the recovery time.
CSMA / CA will first transmit the intent to send for data transmission.	CSMA / CD resends the data frame whenever a conflict occurs.
CSMA / CA is used in 802.11 standard.	CSMA / CD is used in 802.3 standard.
It is similar to simple CSMA(Carrier Sense Multiple Access).	It is more efficient than simple CSMA(Carrier Sense Multiple Access).
It is the type of CSMA to avoid collision on a shared channel.	It is the type of CSMA to detect the collision on a shared channel.
It is work in MAC layer.	It also work in MAC layer.

**49.What is Round Trip Time(RTT)?(APRIL/MAY 2024)**

- RTT (Round Trip Time) also called round-trip delay is a crucial tool in determining the health of a network.
- It is the time between a request for data and the display of that data. It is the duration measured in milliseconds.
- RTT can be analyzed and determined by pinging a certain address. It refers to the time taken by a network request to reach a destination and to revert back to the original source.

**50.What type of switching is used in present digital communication?****Packet switching**

- Packet switching is the primary basis for data communications in computer networks worldwide.
- Packet Switching transmits data across digital networks by breaking it down into blocks or packets for more efficient transfer using various network devices.

**PART B****1. Explain in detail about Network Layer Services.****Synopsis:**

- **Packetizing**
- **Routing and Forwarding**
- **Other Services**

**Packetizing**

- **Packetizing:** encapsulating the payload (data received from upper layer) in a network-layer packet at the source and decapsulating the payload from the network-layer packet at the destination.
- The source host receives the payload from an upper-layer protocol, adds a header that contains the source and destination addresses and some other information that is required by the network-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 decapsulate the packets they received unless the packets need to be fragmented.
- The routers are not allowed to change source and destination addresses either.

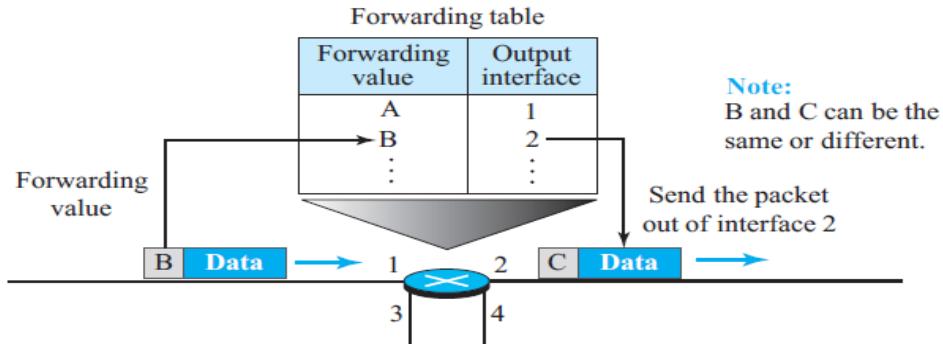
**Routing and Forwarding****Routing**

- The network layer is responsible for routing the packet from its source to the destination.
- A physical network is a combination of networks (LANs and WANs) and routers that connect them.
- The network layer is responsible for finding the best one among these possible routes.

**Forwarding**

- Forwarding can be defined as the action applied by each router when a packet arrives at one of its interfaces.

- The decision-making table a router normally uses for applying this action is 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 or to some attached networks. (Refer fig 3.1)



**Fig 3.1 – Forwarding table**

## Other Services

### 1. Error Control

- The designers of the network layer, however, have added a checksum field to the datagram to control any corruption in the header, but not in the whole datagram.
- This checksum may prevent any changes or corruptions in the header of the datagram.
- The Internet uses an auxiliary protocol, ICMP, that provides some kind of error control if the datagram is discarded or has some unknown information in the header.

### 2. Flow Control

- Flow control regulates the amount of data a source can send without overwhelming the receiver.
- To control the flow of data, the receiver needs to send some feedback to the sender to inform the latter that it is overwhelmed with data.
- The network layer in the Internet, however, does not directly provide any flow control.

### 3. Congestion Control

- Another issue in a network-layer protocol is congestion control. Congestion in the network layer is a situation in which too many datagrams are present in an area of the Internet.

- Congestion may occur if the number of datagrams sent by source computers is beyond the capacity of the network or routers.
- If the congestion continues, sometimes a situation may reach a point where the system collapses and no datagrams are delivered.

#### **4. Quality of Service**

- As the Internet has allowed new applications such as multimedia communication, the quality of service (QoS) of the communication has become more and more important.

#### **5. Security**

- The network layer was designed with no security provision.
- To provide security for a connectionless network layer, we need to have another virtual level that changes the connectionless service to a connection-oriented service. This virtual layer, called IPSec.

## **2. Discuss in detail the concepts of Packet Switched Networks (Packet Switching).**

### **Synopsis:**

<b>SWITCHING</b>
➤ <b>Definition</b>
➤ <b>Type of switching</b>
➤ <b>Advantages of packet switching</b>
<b>PACKET SWITCHING</b>
➤ <b>Datagram approach</b>
➤ <b>The features of datagram</b>
<b>Routing Table</b>
➤ <b>Virtual Circuit Approach</b>
➤ <b>Comparison between Virtual circuit and Datagram</b>
<b>Virtual-Circuit Networks – characteristics</b>
<b>Addressing</b>

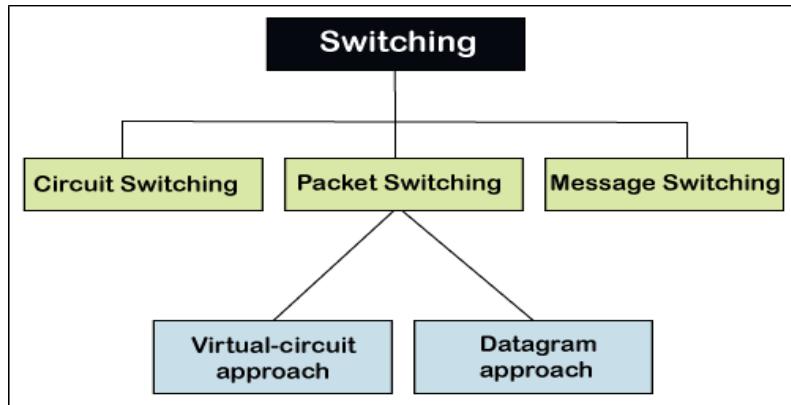
### **Switching**

#### **Definition:**

- To make communication among multiple devices efficiently, a process used is called switching.
- A switched network consists of a series of interlinked nodes called switches.

**Type of switching** (Refer fig 3.2)

- Circuit Switching
- Packet Switching
- Message Switching

**Fig 3.2 – Taxonomy of switched networks****Advantages of packet switching over circuit switching are as follows:**

- Circuit switching is suitable for voice communication. When circuit switched links are used for data transmission, the link is often idle and its facilities wasted.
- The data rate of circuit switched connections for data transmission is very slow.
- Circuit switching is inflexible. Once a circuit has been established, that the path taken by all parts of the transmission whether or not it remains the most efficient.
- Circuit switching treats all transmission as equal. That means, there is no priority among the transmission of data.
- The mostly widely used switching technique for data transmission is packet switching.
- In this, the data are transmitted in the form of packets.
- If the length of the packet is too long then it is broken-up into multiple packets.
- Each packet contains data and also a header with control information.

**Packet switching:**

- There are two popular approaches to packet switching:
  - Datagram approach and
  - Virtual circuit approach

**Datagram Approach:**

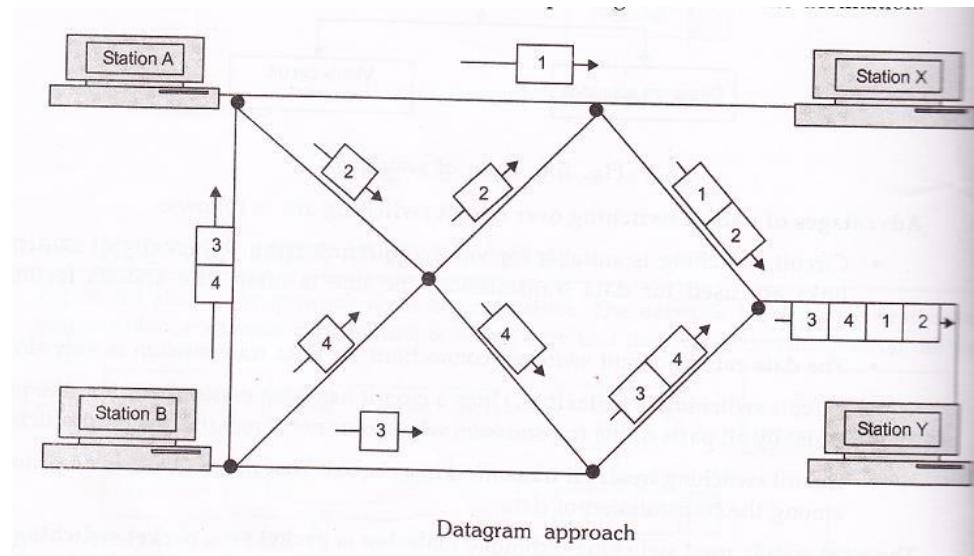
- In the datagram approach, each packet is treated independently from all others.
- A datagram is a multipacket of the same message and it works on the principle of ‘send’ and ‘forget’.

**The features of datagram are as follows:**

- Circuit setup is not needed.
- Each packet contains both source and destination address.
- Each packet routed independently.
- Few packets are lost during crash.
- No effect or router failure.

**Example**

- The below figure shows how the datagram approach can be used to deliver four packets from station A to station Y. (Refer fig 3.3)
- In this example, all four packets belong to the same message but may go by different paths to reach their destination.
- This approach can cause the datagrams of a transmission to arrive at their destination out of order.
- In most protocols, it is the responsibility of transport layer to reorder the datagrams before passing them on to the destination.

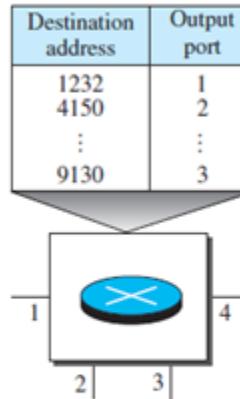


**Fig 3.3 – Datagram approach**

**Routing Table**

- In this type of network, each switch (or packet switch) has a routing table which is based on the destination address.
- The routing tables are dynamic and are updated periodically.
- The destination addresses and the corresponding forwarding output ports are recorded in the tables.

- This is different from the table of a circuit switched network (discussed later) in which each entry is created when the setup phase is completed and deleted when the teardown phase is over (Refer fig 3.4)



A switch in a datagram network uses a routing table that is based on the destination address.

**Fig 3.4 – Routing table in a datagram network**

#### **Virtual Circuit Approach:**

- In the virtual circuit approach, the relationship between all packets belonging to a message or session is preserved.
- A single route is chosen between sender and receiver at the beginning of the session.
- When the data are sent, all packets of the transmission travel one after another along that route.

Virtual circuit transmission is implemented in two formats:

- Switched Virtual Circuit (SVC)
- Permanent Virtual Circuit (PVC)

#### **Switched Virtual Circuit (SVC)**

- In the switched virtual circuit (SVC) method, a virtual circuit is created whenever it is needed exists only for the duration of the specific exchange.
- If the station A wants to send four packets to station X, first it requests the establishment of a connection to station X.
- Once the connection is established, the packets are sent one after another and in sequential order. When the last packet has been received, the connection is released and that virtual circuit ceases to exist.
- Only one single route exists for the duration of transmission. Each time that station A wants to communicate with station X, a new route is established.

**Permanent Virtual Circuit (PVC)**

- In the permanent Virtual Circuit (PVC) method, the same virtual circuit is provided between two users on a continuous basis.
- This circuit is dedicated to the specific users. No one else can use it, because it is always in place.
- It can be used without connection establishment and connection termination.

Two SVC users may get a different route every time they request a connection whereas two PVC users always get the same route.

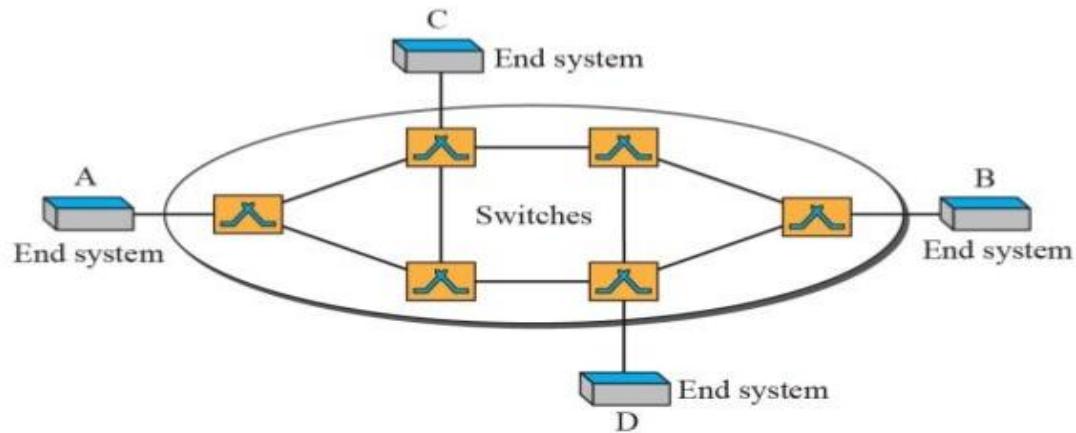
**Comparison between Virtual circuit and Datagram****Table 3.1 – Datagram Vs Virtual circuit**

<b>Datagram approach</b>	<b>Virtual circuit approach</b>
In datagram approach, each packet is treated independently, thus they can follow different routes.	In virtual circuit approach, all packets follow the same route.
Packets can arrive at the destination in different order.	Packets should reach the destination in the same order.
Connection establishment is not required before transmission	Connection establishment is required.

**Virtual-Circuit Networks – characteristics**

- A **virtual-circuit network** is a cross between a circuit-switched network and a datagram network. It has some characteristics of both. (Refer fig 3.5).
  1. As in a circuit-switched network, there are **setup and teardown phases** in addition to the data **transfer phase**.
  2. Resources can be allocated during the setup phase, as in a circuit-switched network, or on demand, as in a datagram network.
  3. As in a datagram network, data are packetized and each packet carries an address in the header. However, the address in the header has local jurisdiction (it defines what the next switch should be and the channel on which the packet is being carried), not end-to-end jurisdiction. The reader may ask how the intermediate switches know where to send the packet if there is no final destination address carried by a packet. The answer will be clear when we discuss virtual-circuit identifiers in the next section.

4. As in a circuit-switched network, all packets follow the same path established during the connection.
5. A virtual-circuit network is normally implemented in the data-link layer, while a circuit-switched network is implemented in the physical layer and a datagram network in the network layer. But this may change in the future.



**Fig 3.5 – Virtual circuit network**

### Addressing

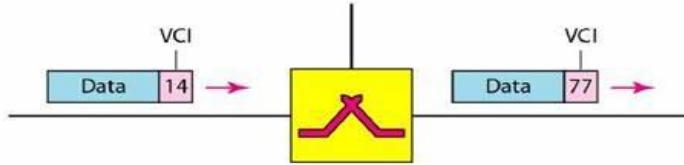
In a virtual-circuit network, two types of addressing are involved: global and local (virtual-circuit identifier).

### Global Addressing

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

### Virtual-Circuit Identifier

- The identifier that is actually used for data transfer is called the **virtual-circuit identifier (VCI)** or the label.
- A VCI, unlike a global address, is a small number that has only switch scope; it is used by a frame between two switches. (Refer fig 3.6)

**Fig 3.6 – Virtual circuit identifier****Three Phases**

- As in a circuit-switched network, a source and destination need to go through three phases in a virtual-circuit network: setup, data transfer, and teardown.
  - In the setup phase, the source and destination use their global addresses to help switches make table entries for the connection.
  - In the teardown phase, the source and destination inform the switches to delete the corresponding entry.
  - Data transfer occurs between these two phases.

**3. Differentiate circuit switching and packet switching with suitable application example (Nov/Dec 2021)****Table 3.2 – Circuit Vs Packet Switching**

<b>Circuit switching</b>	<b>Packet switching</b>
In-circuit switching has three phases: i) Connection Establishment. ii) Data Transfer. iii) Connection Released.	In Packet switching directly data transfer takes place.
In-circuit switching, each data unit knows the entire path address which is provided by the source.	In Packet switching, each data unit just knows the final destination address intermediate path is decided by the routers.
In-Circuit switching, data is processed at the source system only	In Packet switching, data is processed at all intermediate nodes including the source system.
The delay between data units in circuit switching is uniform.	The delay between data units in packet switching is not uniform.
Resource reservation is the feature of circuit switching because the path is fixed for data transmission.	There is no resource reservation because bandwidth is shared among users.

Circuit switching is more reliable.	Packet switching is less reliable.
Wastage of resources is more in Circuit Switching	Less wastage of resources as compared to Circuit Switching
It is not a store and forward technique.	It is a store and forward technique.
Transmission of the data is done by the source	Transmission of the data is done not only by the source but also by the intermediate routers.
Congestion can occur during the connection establishment phase	Congestion can occur during the data transfer phase
Circuit switching is not convenient for handling bilateral traffic.	Packet switching is suitable for handling bilateral traffic.
Recording of packets is never possible in circuit switching.	Recording of packets is possible in packet switching.
In-Circuit Switching there is a physical path between the source and the destination	In Packet Switching there is no physical path between the source and the destination
Call setup is required in circuit switching	No call setup is required in packet switching.
In-circuit switching each packet follows the same route.	In packet switching packets can follow any route.
The circuit switching network is implemented at the physical layer.	Packet switching is implemented at the datalink layer and network layer
Circuit switching requires simple protocols for delivery.	Packet switching requires complex protocols for delivery.

#### 4. Explain the performance of network layer in detail.

**Synopsis:**

➤ **Performance of network layer**

- Delay
- Throughput
- Packet Loss
- Congestion Control

**Performance of network layer:**

- The performance of a network can be measured in terms of
  - delay,
  - throughput,
  - packet loss.
- Congestion control is an issue that can improve the performance.

**1. Delay**

- All of us expect instantaneous response from a network, but a packet, from its source to its destination, encounters delays.
- The delays in a network can be divided into four types:
  - transmission delay,
  - propagation delay,
  - processing delay,
  - queuing delay.

**➤ Transmission Delay**

- A sender needs to put the bits in a packet one by one.
- If the first bit of the packet is put on the line at time  $t_1$  and the last bit is put on the line at time  $t_2$ , transmission delay of the packet is  $(t_2 - t_1)$ .
- The transmission delay is longer for a longer packet and shorter if the sender can transmit faster. In other words, the transmission delay is

$$\text{Delay}_{\text{tr}} = (\text{Packet length}) / (\text{Transmission rate}).$$

**➤ Propagation Delay**

- Propagation delay is the time it takes for a bit to travel from point A to point B in the transmission media.
- The propagation delay depends on the propagation speed of the media, which is  $3 \times 10^8$  meters/second in a vacuum and normally much less in a wired medium; it also depends on the distance of the link.

$$\text{Delay}_{\text{pg}} = (\text{Distance}) / (\text{Propagation speed}).$$

**➤ Processing Delay**

- The processing delay is the time required for a router or a destination host to receive a packet from its input port, remove the header, perform an error detection

procedure, and deliver the packet to the output port (in the case of a router) or deliver the packet to the upper-layer protocol (in the case of the destination host).

**Delay<sub>pr</sub>** = Time required to process a packet in a router or a destination host

#### ➤ Queuing Delay

- The queuing delay for a packet in a router is measured as the time a packet waits in the input queue and output queue of a router.

**Delay<sub>qu</sub>** = The time a packet waits in input and output queues in a router

#### ➤ Total Delay

- If we have n routers, we have (n + 1) links.
- Therefore, we have (n + 1) transmission delays related to n routers and the source, (n + 1) propagation delays related to (n + 1) links, (n + 1) processing delays related to n routers and the destination, and only n queuing delays related to n routers.

**Total delay = (n + 1) (Delay<sub>tr</sub> + Delay<sub>pg</sub> + Delay<sub>pr</sub>) + (n) (Delay<sub>qu</sub>)**

## 2. Throughput

- Throughput at any point in a network is defined as the number of bits passing through the point in a second, which is actually the transmission rate of data at that point.
- In a path from source to destination, a packet may pass through several links (networks), each with a different transmission rate.

**Throughput = minimum {TR1, TR2, . . . TRn}.**

## 3. Packet Loss

- When a router receives a packet while processing another packet, the received packet needs to be stored in the input buffer waiting for its turn.
- A router, however, has an input buffer with a limited size. A time may come when the buffer is full and the next packet needs to be dropped.
- This effect is packet loss.

## 4. Congestion Control

- Congestion control is a mechanism for improving performance.
- Congestion control refers to techniques and mechanisms that can either prevent congestion before it happens or remove congestion after it has happened.
- Two broad categories:
  - open-loop congestion control (prevention)

- closed-loop congestion control (removal).

➤ **Open-Loop Congestion Control**

- In open-loop congestion control, policies are applied to prevent congestion before it happens.
- In these mechanisms, congestion control is handled by either the source or the destination.
- The policies are Retransmission Policy, Window Policy, Acknowledgment Policy, Discarding Policy, Admission Policy.

➤ **Closed-Loop Congestion Control.**

- Closed-loop congestion control mechanisms try to alleviate congestion after it happens.
- Several mechanisms have been used by different protocols.
  - Backpressure
  - Choke Packet
  - Implicit Signalling
  - Explicit Signalling

**5. Explain in detail IPv4 Addresses.?**

**Synopsis:**

**IPV4 ADDRESSES**

1. Address Space
2. Classful Addressing
3. Classless Addressing

**IPV4 ADDRESSES**

- The identifier used in the IP layer of the TCP/IP protocol suite to identify the connection of each device to the Internet is called the Internet address or IP address.
- The IP address is the address of the connection, not the host or the router, because if the device is moved to another network, the IP address may be changed.
- An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a host or a router to the Internet.

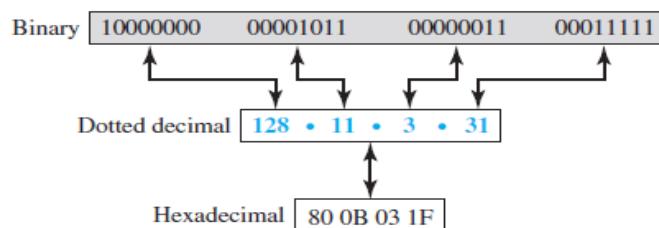
- IPv4 addresses are unique. If a device has two connections to the Internet, via two networks, it has two IPv4 addresses.

### 1. Address Space

- A protocol like IPv4 that defines addresses has an address space.
- An address space is the total number of addresses used by the protocol.
- IPv4 uses 32-bit addresses, which means that the address space is  $2^{32}$  or 4,294,967,296 (more than four billion)

#### Notation

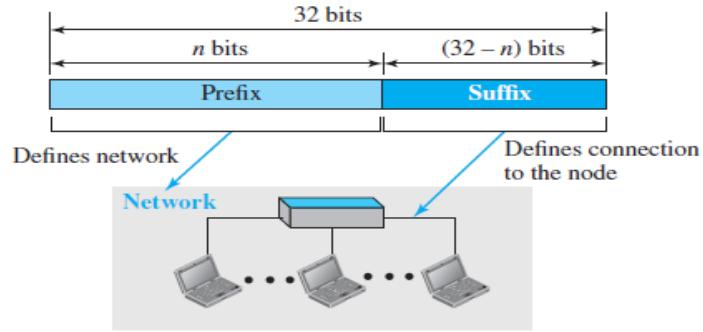
- There are three common notations to show an IPv4 address: binary notation (base 2), dotted-decimal notation (base 256), and hexadecimal notation (base 16). (Refer fig 3.7)
- In binary notation, an IPv4 address is displayed as 32 bits.
- Dotted-decimal notation is decimal point (dot) separating the bytes.
- IPv4 address in hexadecimal notation. Each hexadecimal digit is equivalent to four bits. This means that a 32-bit address has 8 hexadecimal digits.



**Fig 3.7 – Notation**

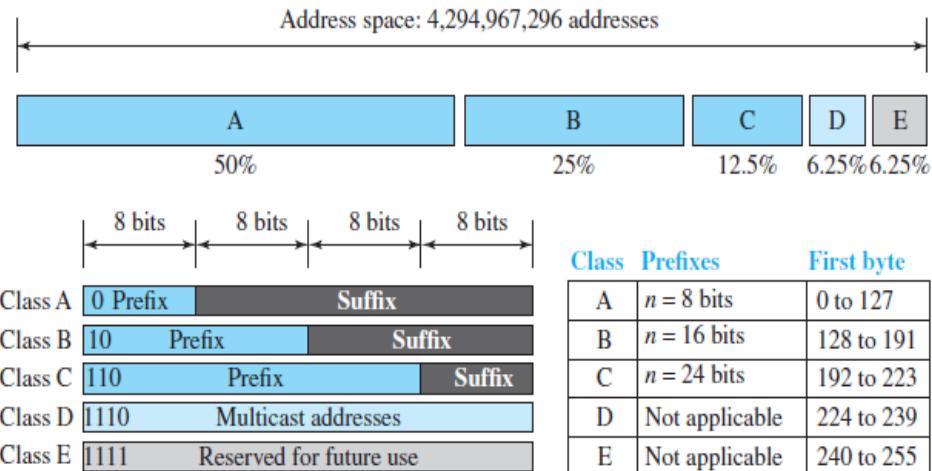
#### Hierarchy in Addressing

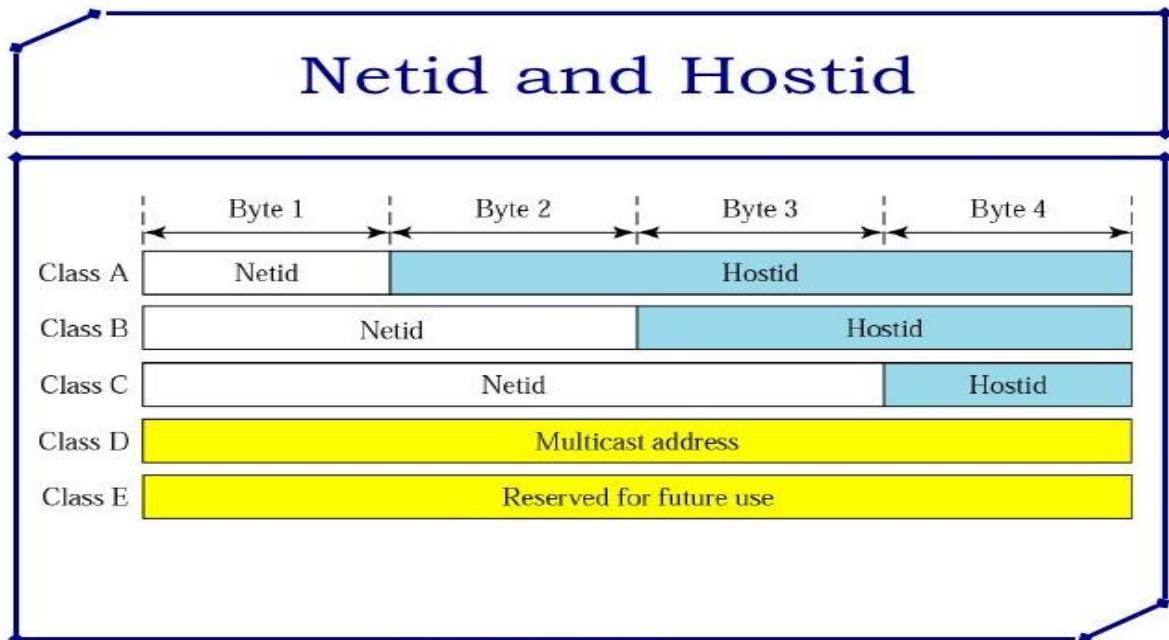
- A 32-bit IPv4 address is also hierarchical, but divided only into two parts. The first part of the address, called the prefix, defines the network; the second part of the address, called the suffix, defines the node (connection of a device to the Internet).
- The prefix length is  $n$  bits and the suffix length is  $(32 - n)$  bits. A prefix can be fixed length or variable length. (Refer fig 3.8)

**Fig 3.8 – Address space**

## 2. Classful Addressing

An IPv4 address was designed with a fixed-length prefix. The whole address space was divided into five classes (class A, B, C, D, and E). This scheme is referred to as classful addressing. (Refer fig 3.9 & 3.10)

**Fig 3.9 – IPv4 classes**

**Fig 3.10 – Netid and hostid**

- Addresses in classes A, B and C are for unicast communication, from one source to one destination.
- Addresses in class D are for multicast communication, from one source to a group of destination. A multicast address is used only in destination addresses.
- Addresses in class E are reserved. The original idea was to use them for special purpose.

### **Subnetting and Supernetting**

- To alleviate address depletion, two strategies were proposed and implemented: subnetting and supernetting.
- In subnetting, a class A or class B block is divided into several subnets. Each subnet has a larger prefix length than the original network.
- Subnetting allows the addresses to be divided among several organizations.
- Supernetting was devised to combine several class C blocks into a larger block to be attractive to organizations that need more than the 256 addresses available in a class C block.

### **Advantage of Classful Addressing**

Given an address, we can easily find the class of the address and, since the prefix length for each class is fixed, we can find the prefix length immediately.

**Examples:**

1. Find the class for the following IP addresses.  
(i) 205.55.43.11 and  
(ii) 100.23.28.65

**Solution:**

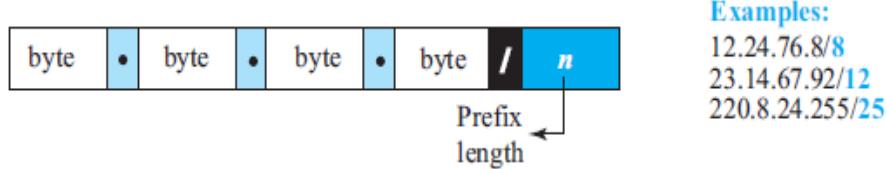
- i) Class C (First byte 205 between 192 to 223)  
ii) Class A (First byte 100 between 0 to 127)
2. Find the class for the following IP address:
  - i) 11110111 11110010 10000011 10101010 - Class E (First byte starts with 1111)
  - ii) 01111111 11110000 01010111 00001100 - Class A (First byte starts with 0)
3. Find the netid and hostid for the following:
  - i) 19.34.1.5 - netid = 19 hostid = 34.1.5
  - ii) 190.3.70.10 - netid = 190.3 hostid = 70.10
  - iii) 246.3.4.10 - No netid and no hostid because 246.3.4.10 is the class E address.
  - i) 201.2.4.2 - netid = 201.2.4 hostid = 2

**3. Classless Addressing**

- In addressing, the whole address space is divided into variable length classless blocks.
- The prefix in an address defines the block (network); the suffix defines the node (device).
- A prefix length ranges from 0 to 32. The size of the network is inversely proportional to the length of the prefix. A small prefix means a larger network; a large prefix means a smaller network.

**Prefix Length: Slash Notation**

- The prefix length, n, is added to the address, separated by a slash.
- The notation is informally referred to as slash notation and formally as classless interdomain routing or CIDR strategy. (Refer fig 3.11)
- An address in classless addressing can then be represented as shown in

**Fig 3.11 – Prefix Length****Address Mask**

- The address mask is a 32-bit number in which the n leftmost bits are set to 1s and the rest of the bits ( $32 - n$ ) are set to 0s.
- To extract the information in a block, using the three bit-wise operations NOT, AND, and OR.
  1. The number of addresses in the block  $N = \text{NOT}(\text{mask}) + 1$ .
  2. The first address in the block = (Any address in the block) AND (mask).
  3. The last address in the block = (Any address in the block) OR [(NOT (mask))].

**Network Address**

- The network address is actually the identifier of the network; because it is used in routing a packet to its destination network.

**6. Explain the forwarding of IP packets in detail.****Synopsis:****FORWARDING OF IP PACKETS**

- Forwarding Based on Destination Address
- Forwarding Based on Label
- Routers as Packet Switches

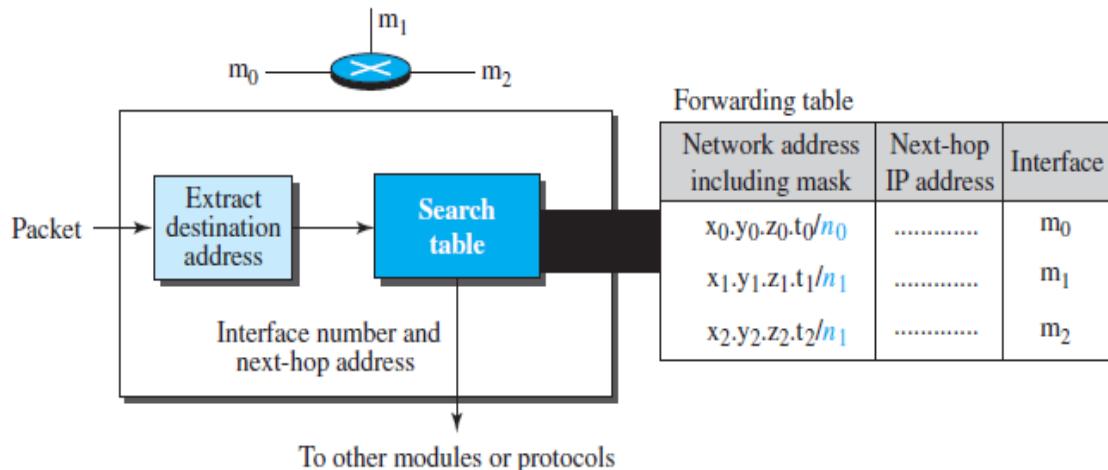
**➤ FORWARDING OF IP PACKETS**

- Forwarding means to place the packet in its route to its destination.
- When IP is used as a connectionless 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.

**➤ Forwarding Based on Destination Address**

- 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.
- The table needs to be searched based on the network address.
- 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.
- 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. (Refer fig 3.12)
- 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 3.12 – Forward of IP packets**

#### ➤ **Forwarding Based on Label**

- In a connection-oriented network (virtual-circuit approach), a switch forwards a packet based on the label attached to the packet.
- When the forwarding algorithm gets the destination address of the packet, 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.

#### ➤ **Routers as Packet Switches**

- The packet switches that are used in the network layer are called routers.
- Routers can be configured to act as either a datagram switch or a virtual-circuit switch.

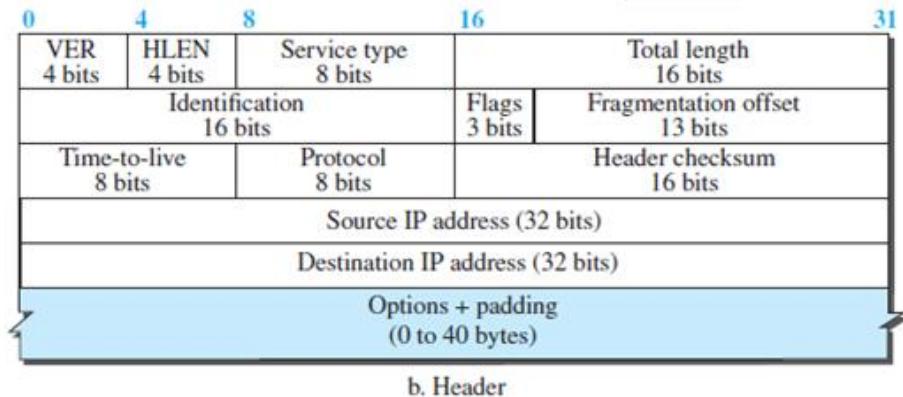
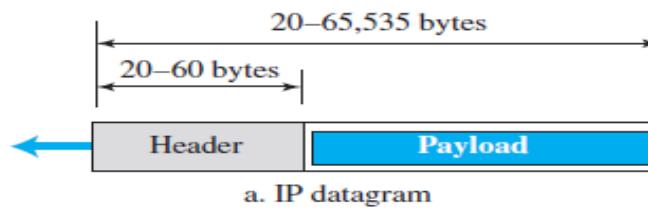
**7. Explain about INTERNET PROTOCOL (IP) in detail (or) Illustrate IPV4 header format and compare with IPv6 (Nov 2021).**

➤ **INTERNET PROTOCOL (IP)**

- The Internet Protocol version 4 (IPv4), is responsible for packetizing, forwarding, and delivery of a packet at the network layer.

**Datagram Format**

- Packets used by the IP are called **datagrams**.
- A datagram is a variable-length packet consisting of two parts: header and payload (data).
- The header is 20 to 60 bytes in length and contains information essential to routing and delivery. (Refer fig 3.13)



**Fig 3.13 – IP header format**

- **Version Number.**
  - The 4-bit version number (VER) field defines the version of the IPv4 protocol, which, obviously, has the value of 4.
- **Header Length.**
  - The 4-bit header length (HLEN) field defines the total length of the datagram header in 4-byte words. The IPv4 datagram has a variable-length header.

- **Service Type.**
  - Type of service (TOS), defines how the datagram should be handled.
- **Total Length.**
  - This 16-bit field defines the total length (header plus data) of the IP datagram in bytes.
- **Identification, Flags, and Fragmentation Offset.**
  - These three fields are related to the fragmentation of the IP datagram when the size of the datagram is larger than the underlying network can carry.
- **Time-to-live.**
  - The time-to-live (TTL) field is used to control the maximum number of hops (routers) visited by the datagram. When a source host sends the datagram, it stores a number in this field.
  - Each router that processes the datagram decrements this number by one. If this value, after being decremented, is zero, the router discards the datagram.
- **Protocol.**
  - In TCP/IP, the data section of a packet, called the payload, carries the whole packet from another protocol.
  - A datagram, for example, can carry a packet belonging to any transport-layer protocol such as UDP or TCP.
- **Header checksum.**
  - IP adds a header checksum field to check the header for error control, but not the payload.
  - Since the value of some fields, such as TTL, which are related to fragmentation and options, may change from router to router, the checksum needs to be recalculated at each router.
- **Source and Destination Addresses.**
  - These 32-bit source and destination address fields define the IP address of the source and destination respectively.
  - The source host should know its IP address.
  - The destination IP address is either known by the protocol that uses the service of IP or is provided by the DNS.

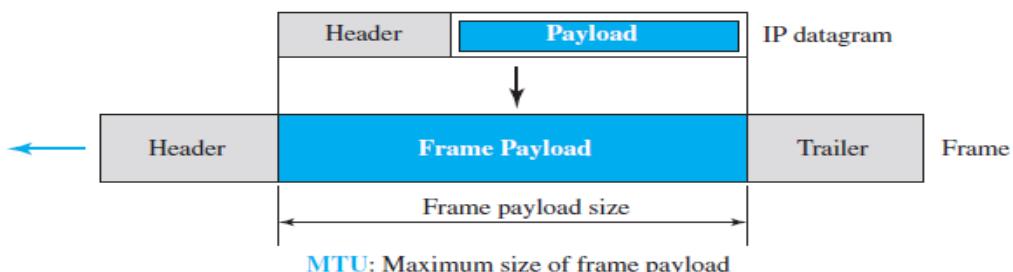
- **Options.**
  - A datagram header can have up to 40 bytes of options. Options can be used for network testing and debugging.
- **Payload.**
  - Payload is the packet coming from other protocols that use the service of IP.

### ➤ **Fragmentation**

- The division of a packet into smaller units to accommodate a protocol's MTU.

#### **Maximum Transfer Unit (MTU)**

- The largest size data unit a specific network can handle.



**Fig 3.14 – MTU**

- The value of the MTU differs from one physical network protocol to another.
- When a datagram is fragmented, each fragment has its own header with most of the fields repeated, but some have been changed.
- A datagram may be fragmented several times before it reaches the final destination.
- The host or router that fragments a datagram must change the values of three fields: flags, fragmentation offset, and total length. (Refer fig 3.14).

#### **Three fields in an IP datagram are related to fragmentation:**

identification, flags, and fragmentation offset.

- The 16-bit identification field identifies a datagram originating from the source host.
- The 3-bit flags field defines three flags.
  - The leftmost bit is reserved (not used).
  - The second bit (D bit) is called the do not fragment bit.
    - If its value is 1, the machine must not fragment the datagram.
    - If its value is 0, the datagram can be fragmented if necessary.
  - The third bit (M bit) is called the more fragment bit.

- If its value is 1, it means the datagram is not the last fragment; there are more fragments after this one.
- If its value is 0, it means this is the last or only fragment.
- The 13-bit fragmentation offset field shows the relative position of this fragment with respect to the whole datagram.
- 

**8. Explain about Internet Control Message Protocol version 4 (ICMPv4) in detail.(April/may2024)**

**ICMPv4**

- MESSAGES
- Debugging Tools
- ICMP Checksum

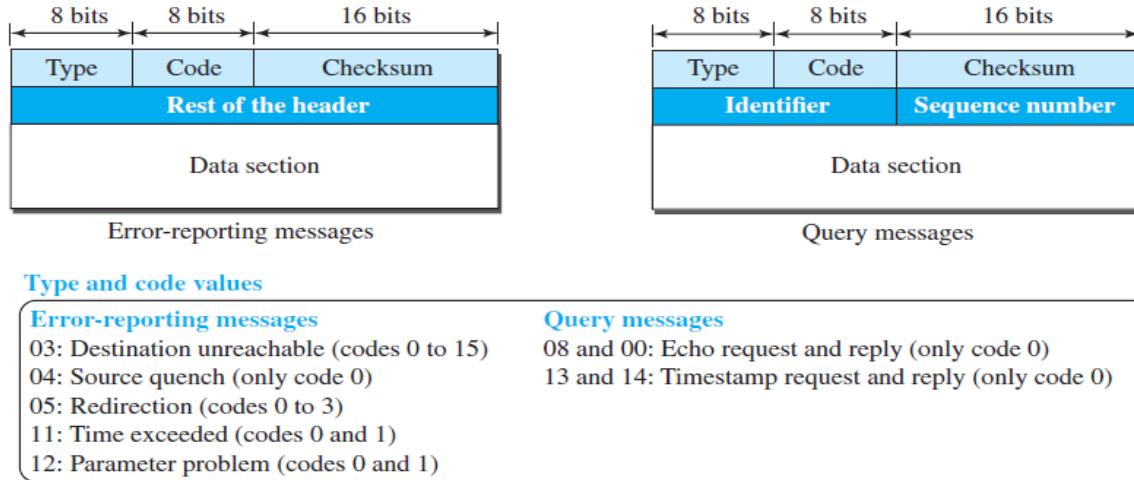
- The Internet Control Message Protocol version 4 (ICMPv4) helps IPv4 to handle some errors that may occur in the network-layer delivery.
- ICMP is used to report some errors that may occur during the processing of the IP datagram.
- ICMP does not correct errors, it simply reports them.

➤ **MESSAGES**

- ICMP messages are divided into two broad categories: (Refer fig 3.15)

**error-reporting messages and query messages**

- An ICMP message has an 8-byte header and a variable-size data section.
- The first field, ICMP type, defines the type of the message.
- The code field specifies the reason for the particular message type.
- The last common field is the checksum field.
- The rest of the header is specific for each message type.
- The data section in error messages carries information for finding the original packet that had the error.
- In query messages, the data section carries extra information based on the type of query.

**Fig 3.15 – ICMPv4 messages**

### Error Reporting Messages

- The error-reporting messages report problems that a router or a host (destination) may encounter when it processes an IP packet.
- To make the error-reporting process simple, ICMP follows some rules in reporting messages.
  - First, no error message will be generated for a datagram having a multicast address or special address (such as this host or loopback).
  - Second, no ICMP error message will be generated in response to a datagram carrying an ICMP error message.
  - Third, no ICMP error message will be generated for a fragmented datagram that is not the first fragment.

#### 1. Destination Unreachable

- The most widely used error message is the destination unreachable (type 3).
- This message uses different codes (0 to 15) to define the type of error message and the reason why a datagram has not reached its final destination.

#### 2. Source Quench

- It informs the sender that the network has encountered congestion and the datagram has been dropped; the source needs to slow down sending more datagrams.

#### 3. Redirection Message

- The redirection message (type 5) is used when the source uses a wrong router to send out its message.

- The router redirects the message to the appropriate router, but informs the source that it needs to change its default router in the future.

#### 4. Time Exceeded

- When the TTL value becomes 0, the datagram is dropped by the visiting router and a time exceeded message (type 11) with code 0 is sent to the source to inform it about the situation.
- The time-exceeded message (with code 1) can also be sent when not all fragments of a datagram arrive within a predefined period of time.

#### 5. Parameter Problem

- A parameter problem message (type 12) can be sent when either there is a problem in the header of a datagram (code 0) or some options are missing or cannot be interpreted (code 1).

### Query Messages

- Query messages are used to probe or test the liveliness of hosts or routers in the Internet.
- The query messages come in pairs: request and reply.
- The echo request (type 8) and the echo reply (type 0) pair of messages are used by a host or a router to test the liveliness of another host or router.
- A host or router sends an echo request message to another host or router; if the latter is alive, it responds with an echo reply message.

### ➤ Debugging Tools

- Two debugging tools: ping and traceroute.

#### Ping

- Ping program is used to find if a host is alive and responding.
- The source host sends ICMP echo-request messages; the destination, if alive, responds with ICMP echo-reply messages.
- The ping program gets help from two query messages;

#### Traceroute or Tracert

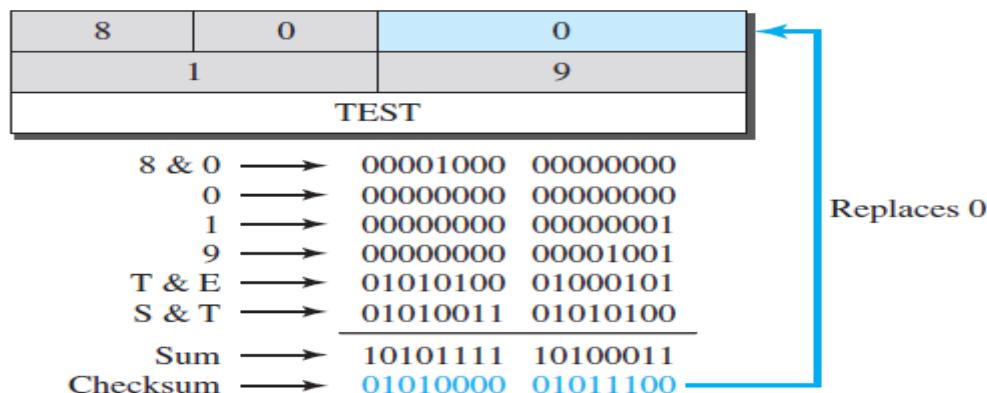
- The traceroute program in UNIX or tracert in Windows can be used to trace the path of a packet from a source to the destination.
- It can find the IP addresses of all the routers that are visited along the path.
- The traceroute program gets help from two error-reporting messages: time-exceeded and destination-unreachable.

➤ **ICMP Checksum**

- In ICMP the checksum is calculated over the entire message (header and data).

**Example**

An example of checksum calculation for a simple echo-request message. We randomly chose the identifier to be 1 and the sequence number to be 9. The message is divided into 16-bit (2-byte) words. The words are added and the sum is complemented. Now the sender can put this value in the checksum field. (Refer fig 3.16)

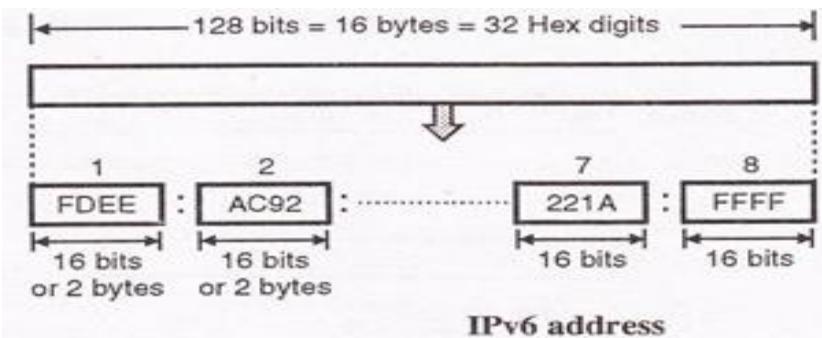


**Fig 3.16 – checksum example**

**9. Explain in detail about IPv6 ADDRESSING & Compare with IPv4 (Nov 2021).**

➤ **IPv6 ADDRESSING**

- The main reason for migration from IPv4 to IPv6 is the small size of the address space in IPv4.
- An IPv6 address is 128 bits or 16 bytes (octets) long, four times the address length in IPv4. (Refer fig 3.17)



**Fig 3.17 – Address length in IPv6.**

➤ **Representation / Notations**

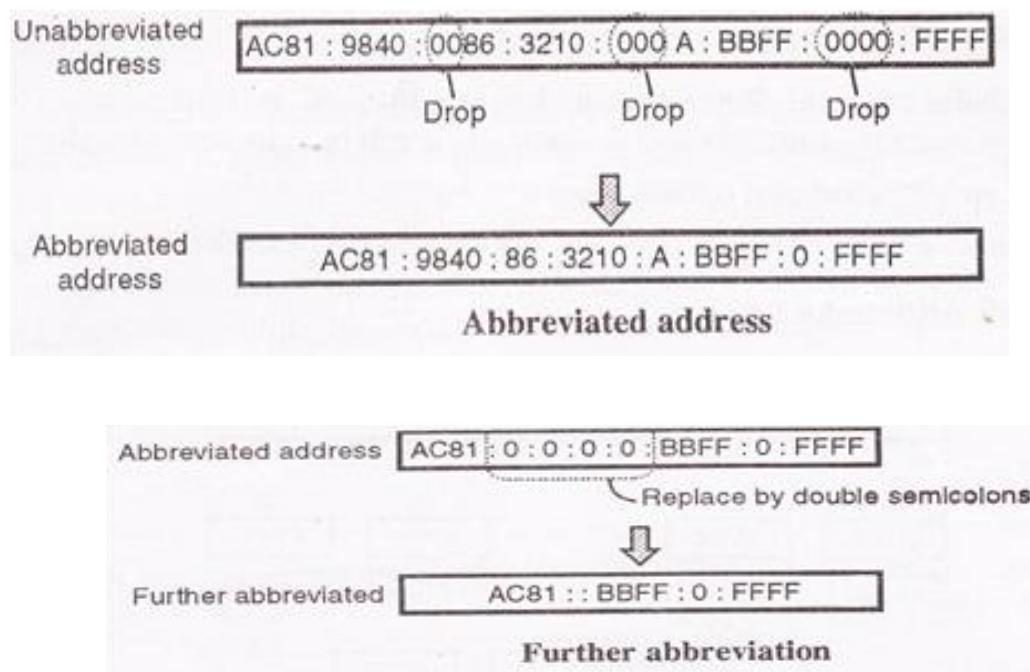
- Binary notation is used when the addresses are stored in a computer.
- The **colon hexadecimal notation** divides the address into eight sections, each made of four hexadecimal digits separated by colons.

Binary (128 bits)	1111111011110110 ... 111111100000000
Colon Hexadecimal	FEF6:BA98:7654:3210:ADEF:BBFF:2922:FF00

**Abbreviation :**

**Zero Compression**

- The IPv6 address, even in hexadecimal format is very long. But in this address there are many of the zero digits in it. In such a case, we can abbreviate the address. The leading zeros of a section (four digits between two colons) can be omitted. (Refer fig 3.18)
- Note that only the leading zeros can be dropped but the trailing zeros cannot drop.



**Fig 3.18 – Abbreviated address IPv6.**

**Mixed Notation**

- Mixed representation of an IPv6 address: colon hex and dotted decimal notation.

- This is appropriate during the transition period in which an IPv4 address is embedded in an IPv6 address (as the rightmost 32 bits).
- For example, the address (::130.24.24.18) is a legitimate address in IPv6.

### CIDR Notation

- IPv6 uses hierarchical addressing. For this, IPv6 allows slash or CIDR notation.
- For example, the following shows how we can define a prefix of 60 bits using CIDR.

**FDEC::BBFF:0:FFFF/60**

### ➤ Address Space

- The address space of IPv6 contains 2<sup>128</sup> addresses. This address space is 2<sup>96</sup> times the IPv4 address.

### Three Address Types

- In IPv6, a destination address can belong to one of three categories:
  - Unicast.
  - Anycast.
  - multicast.

#### 1. Unicast Address

- A unicast address defines a single interface (computer or router).
- The packet sent to a unicast address will be routed to the intended recipient.

#### 2. Anycast Address

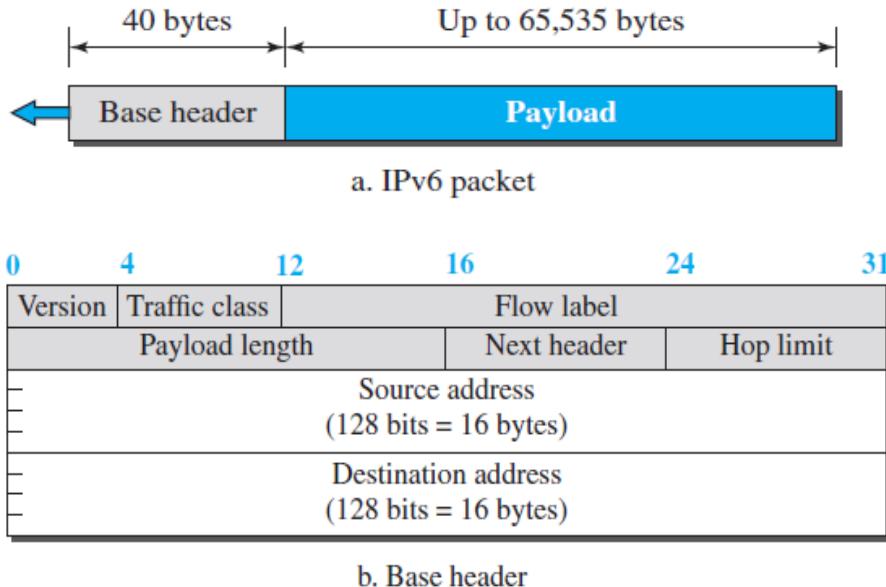
- An **anycast address** defines a group of computers that all share a single address.
- A packet with an anycast address is delivered to only one member of the group, the most reachable one.

#### 3. Multicast Address

- A multicast address also defines a group of computers.
- In multicasting each member of the group receives a copy.

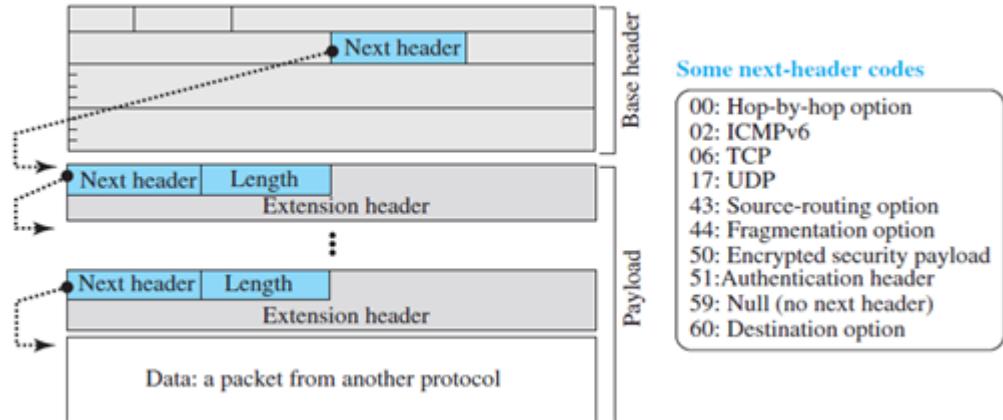
### ➤ IPv6 Packet Format:

- Each packet is composed of a base header followed by the payload.
- The base header occupies 40 bytes, whereas payload can be up to 65,535 bytes of information. (Refer fig 3.19)

**Fig 3.19 – IPv6 Packet Format**

- **Version.** The 4-bit version field defines the version number of the IP. For IPv6, the value is 6.
- **Traffic class.** The 8-bit traffic class field is used to distinguish different payloads with different delivery requirements. It replaces the type-of-service field in IPv4.
- **Flow label.** The flow label is a 20-bit field that is designed to provide special handling for a particular flow of data. We will discuss this field later.
- **Payload length.** The 2-byte payload length field defines the length of the IP datagram excluding the header.
- **Hop limit.** The 8-bit hop limit field serves the same purpose as the TTL field in IPv4.
- **Source and destination addresses.** The source address field is a 16-byte (128-bit) Internet address that identifies the original source of the datagram. The destination address field is a 16-byte (128-bit) Internet address that identifies the destination of the datagram.
- **Payload.** Compared to IPv4, the payload field in IPv6 has a different format and meaning. (Refer fig 3.20)
- The payload in IPv6 means a combination of zero or more extension headers (options) followed by the data from other protocols (UDP, TCP, and so on). Each

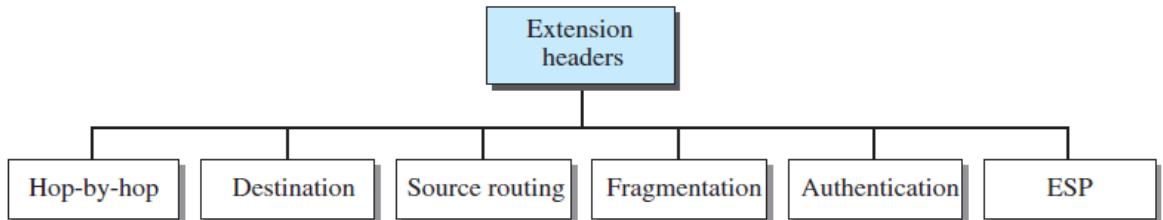
extension header has two mandatory fields, next header and the length, followed by information related to the particular option.



**Fig 3.20 – payload in an IPv6 datagram**

#### ➤ Extension Header

- An IPv6 packet is made of a base header and some extension headers.
- The length of the base header is fixed at 40 bytes. (Refer fig 3.21)
- Extension headers are hop-by-hop option, source routing, fragmentation, authentication, encrypted security payload, and destination option.



**Fig 3.21 – Extension Header**

#### Hop-by-Hop Option

- The hop-by-hop option is used when the source needs to pass information to all routers visited by the datagram.
- Only three hop-by-hop options have been defined:
  - Pad1, PadN, and jumbo payload.
- Pad1. This option is 1 byte long and is designed for alignment purposes.
- PadN. PadN is used when 2 or more bytes are needed for alignment.
- Jumbo payload. Length of the payload in the IP datagram can be a maximum of 65,535 bytes.

**Destination Option**

- The destination option is used when the source needs to pass information to the destination only.
- The format of the destination option is the same as the hop-by-hop option.

**Source Routing**

- The source routing extension header combines the concepts of the strict source route and the loose source route options of IPv4.

**Fragmentation**

- The concept of fragmentation in IPv6 is the same as that in IPv4.
- In IPv6, only the original source can fragment.

**Authentication**

- The authentication extension header has a dual purpose: it validates the message sender and ensures the integrity of data.

**Encrypted Security Payload**

- The encrypted security payload (ESP) is an extension that provides confidentiality and guards against eavesdropping.

**➤ Advantages of IPv6:**

- **Larger address space**
  - IPv6 has 128-bit address space, which is 4 times wider in bits in compared to IPv4's 32-bit address space.
- **Better header format**
  - IPv6 uses a better header format. In its header format the options are separated from the base header.
- **New option**
  - New options have been added in IPv6 to increase the functionality.
- **Possibility of extension**
  - IPv6 has been designed in such a way that there is a possibility of extension of protocol if required.
- **More security**
  - IPv6 includes security in the basic specification.
  - It includes encryption of packets (ESP: Encapsulated Security

Payload) and authentication of the sender of packets (AH: Authentication Header).

- **Support to resource allocation**

- To implement better support for real time traffic (such as video conference), IPv6 includes flow label in the specification.
- With flow label mechanism, routers can recognize to which end-to-end flow the packets belong.

- **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 the network, it will be done automatically.

- **Clearer specification and optimization**

- IPv6 follows good practices of IPv4, and rejects minor flaws/obsolete items of IPv4.

➤ **Comparison of Options between IPv4 and IPv6**

- The no-operation and end-of-option options in IPv4 are replaced by Pad1 and PadN options in IPv6.
- The record route option is not implemented in IPv6 because it was not used.
- The timestamp option is not implemented because it was not used.
- The source route option is called the source route extension header in IPv6.
- The fragmentation fields in the base header section of IPv4 have moved to the fragmentation extension header in IPv6.
- The authentication extension header is new in IPv6.
- The encrypted security payload extension header is new in IPv6.

**10. Explain the concepts of ARP & its frame format.(April/may 2023)****Synopsis:****➤ Address Resolution Protocol (ARP)**

- Introduction
- IP address
- MAC address
- Mapping of IP address into a MAC address
- Static Mapping
- Dynamic mapping
- ARP Operation
- ARP Packet Format

**Address Resolution Protocol (ARP)****Introduction**

- An internet consists of various types of networks and the connecting devices like routers.
- A packet starts from the source host, passes through many physical networks and finally reaches the destination host.
- At the network level, the hosts and routers are recognized by their IP addresses.

**IP address**

- An IP address is an internetwork address. It is a universally unique address.
- Every protocol involved in internetworking requires IP addresses.

**MAC address**

- The packets from source to destination hosts pass through physical networks.
- At the physical level the IP address is not useful but the hosts and routers are recognized by their MAC addresses.
- A MAC address is a local address. It is unique locally but it is not unique universally.
- The IP and MAC address are two different identifiers and both of them are needed
- Deliver a packet to a host or a router, we require two levels of addressing namely IP addressing and MAC addressing.

- Most importantly we should be able to map the IP address into a corresponding MAC address.

### **Mapping of IP address into a MAC address**

- We have seen the need of mapping an IP address into a MAC address.
- Two types of mapping 1) Static mapping and 2) Dynamic mapping.

#### **Static Mapping**

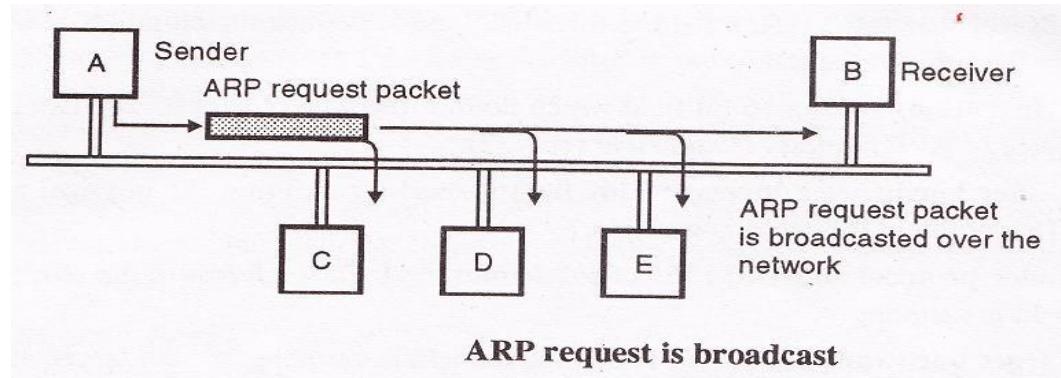
- In static mapping a table is created and stored in each machine. This table associates an IP address with a MAC address.
- If a machine knows the IP address of another machine then it can search for the corresponding MAC address in its table.
- The limitation of static mapping is that the MAC addresses can change.
- To implement static mapping, the static mapping table needs to be updated periodically.

#### **Dynamic mapping**

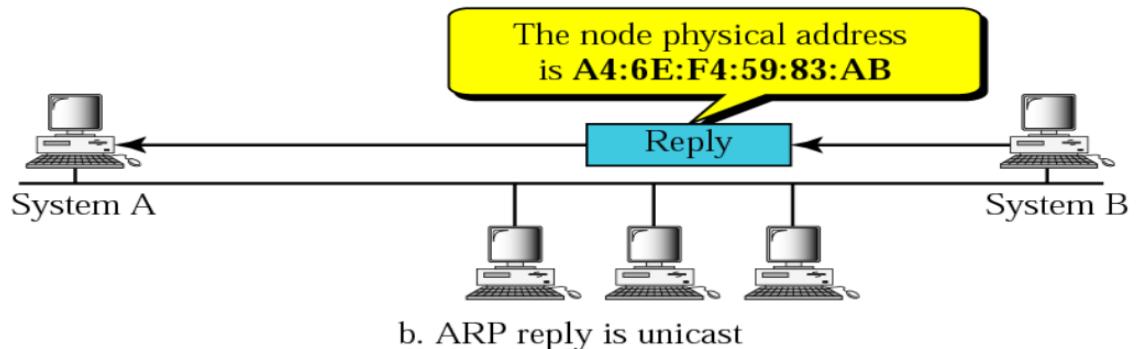
- In dynamic mapping technique a protocol is used for finding the other address when one type of address is known.
- There are two type of dynamic mapping available.
  - Address Resolution Protocol (ARP)
  - Reverse Address Resolution Protocol (RARP)
- The ARP maps IP address to a MAC address whereas the RARP maps a MAC address to an IP address.

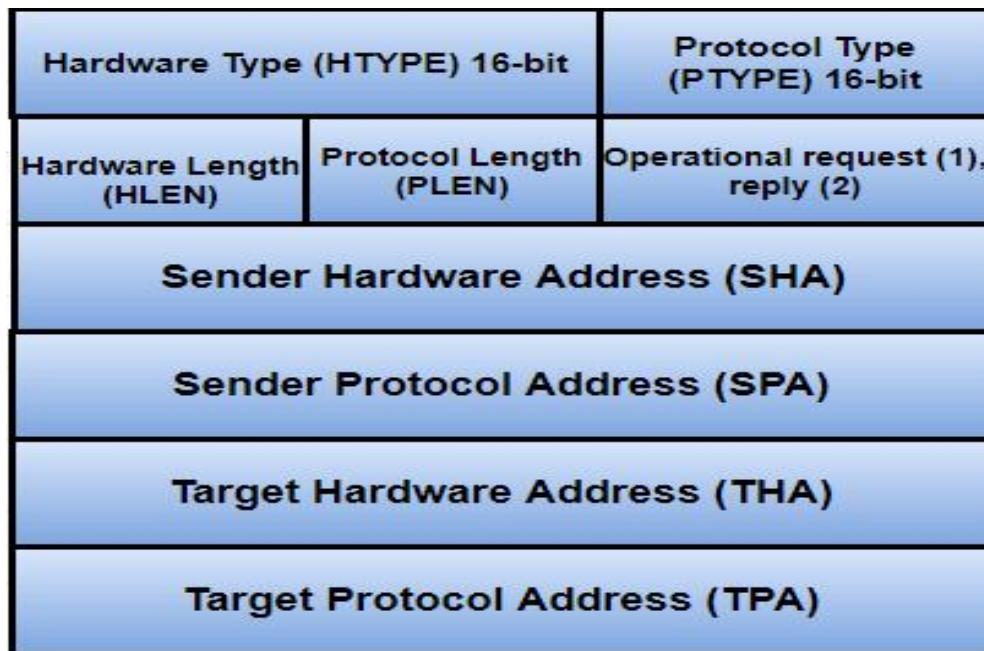
#### **ARP Operation**

- ARP is used for **associating an IP address to its MAC address**.
- For a LAN, each device has its own physical or station address as its identification. This address is imprinted on the NIC.
- Find the MAC address:
- When a router or a host needs to find the MAC address of another host or network the sequence of events taking place is as follows: (Refer fig 3.22)
  - a. The router or a host A who wants to find the MAC address of some other router, sends an ARP request packet. This packet consists of IP and MAC addresses of the sender A and the IP address of the receiver (B).
  - b. This request packet is broadcasted over the network as shown the figure.

**Fig 3.22 – ARP request**

- Every host and router on the network receives and processes the ARP request packet. But only the intended receiver (B) recognizes its IP address in the request packet and sends back an ARP response packet.
- The ARP response packet contains the IP and physical addresses of the receiver (B). This packet is delivered only to A (unicast) using A's physical address in the ARP request packet. This is shown in the following figure. (Refer fig 3.23)

**Fig 3.23 – ARP response**

**ARP Packet Format:****Fig 3.24 – ARP Packet format****HTYPE (Hardware type):**

- This 16 bit field defines the type of network on which is ARP is being run. ARP can run on any physical network. (Refer fig 3.24).

**PTYPE (Protocol type):**

- This 16 bit field is used to define the protocol using ARP. Note that ARP can be used with any higher-level protocol such as IPv4.

**HLEN (Hardware length):**

- It is an 8 bit field which is used for defining the length of the physical address in bytes.
- For example, this value is 6 for Ethernet.

**PLEN (Protocol length):**

- This field is 8 bit long and it defines the length of the IP address in bytes. For IPv4 this value is 4.

**OPER (Operation):**

- It is a 16 bit field which defines the type of packet. The two possible types of packets are:
  - ✓ ARP request (1) and ARP reply (2).

**SHA (Sender Hardware Address):**

- This field is used for defining the physical address of the sender. The length of this field is variable.

**SPA (Sender Protocol address):**

- This field defines the logical address of the sender. The length of this field is variable.

**THA (Target hardware address):**

- It defines the physical address of the target. It is a variable length field.
- For the ARP request packet, this field contains all zeros because the sender does not know the receiver's physical address.

**TPA (Target Protocol address):**

- This field defines the logical address of the target. It is a variable length field.

**11. Explain the concepts of RARP & its frame format.(April/may 2023)**➤ **Synopsis:**

- **RARP – Reverse ARP**
- **Difference between ARP and RARP**

**RARP – Reverse ARP**

- Reverse Address Resolution protocol (RARP) allows a host to convert its MAC address to the corresponding IP address.
- Reverse Address Resolution Protocol (RARP) is a network-specific standard protocol.
- It is described in RFC 903. Some network hosts, such as a diskless workstation, do not know their own IP address when they are booted.
- To determine their own IP address, they use a mechanism similar to ARP, but now the hardware address of the host is the known parameter, and the IP address is the queried parameter. (Refer fig 3.25)
- The reverse address resolution is performed the same way as the ARP address resolution.
- The same packet format is used for the ARP. (Refer fig 3.26)

An exception is the operation code field that now takes the following values–

- 3 for RARP request
- 4 for RARP reply

- The physical header of the frame will now indicate RARP as the higher-level protocol (8035 hex) instead of ARP (0806 hex) or IP-(0800 hex) in the Ether type field.

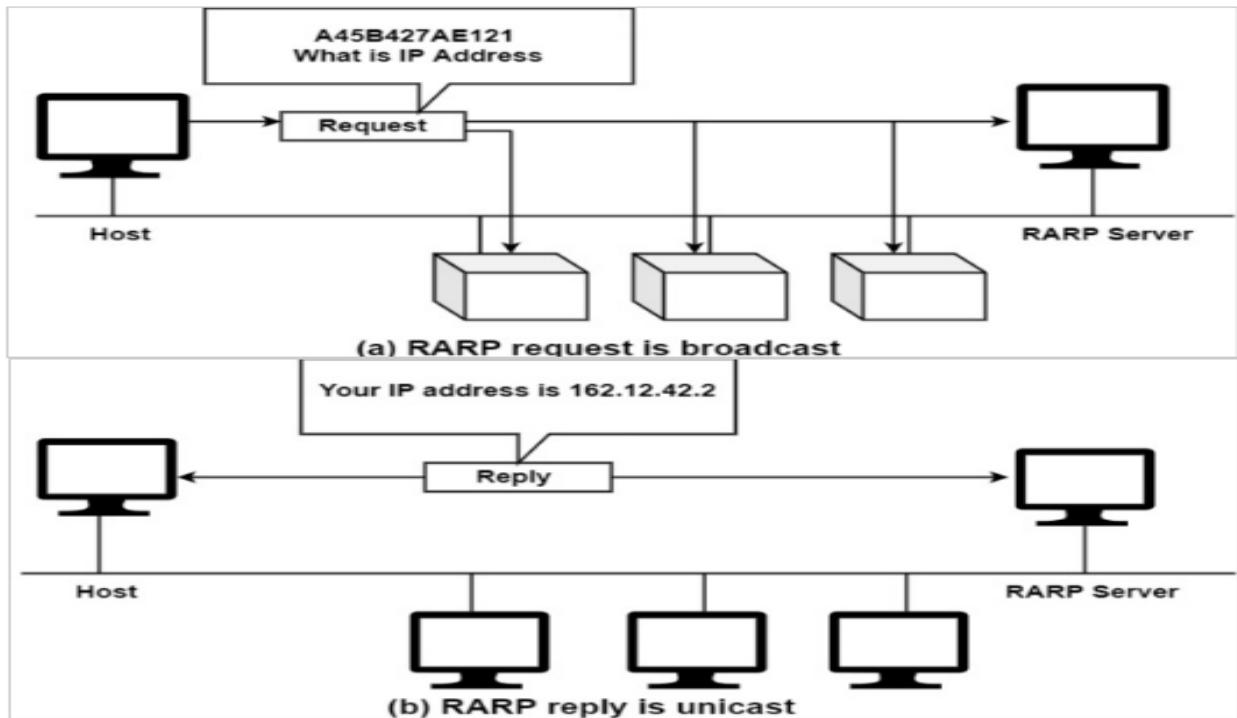
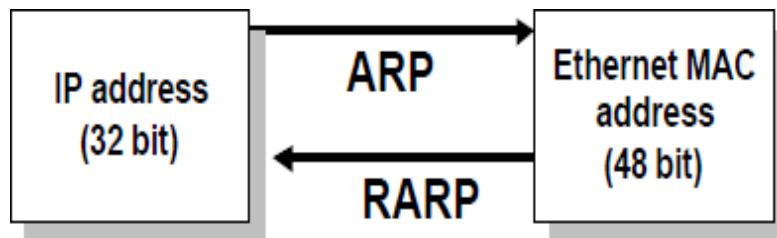


Fig 3.25– RARP

**Difference between ARP and RARP**

<b>Basic</b>	<b>ARP</b>	<b>RARP</b>
<b>Definition</b>	The Internet Protocol(IP) address of the host is mapped with MAC address of the client or server.	The MAC address of the server is mapped to the Internet Protocol address of the client.
<b>IP Address</b>	ARP will help to find the IP address of the different systems.	RARP will help to find the IP address of the same system.
<b>Maintenance</b>	The ARP table is maintained or managed by the local host.	The RARP table is maintained or managed on the server side.
<b>LAN Transmission</b>	A Broadcast MAC address is used.	A Broadcast IP address is used.
<b>Purpose</b>	It is used to get the Machine address of a system using its Internet Protocol address.	The layer 2 forwarding tables are updated by RARP whenever a MAC address changes data centers.
<b>Common Improvements</b>	We need to maintain a cache of recent translations and the storage space required for these addresses is small. So store the IP and physical addresses of every host that broadcasts ARP. Every host	RARP clients should not be allowed to keep trying. That only results in useless broadcasts and so has one or two RARP backup servers running at arbitrary delays.

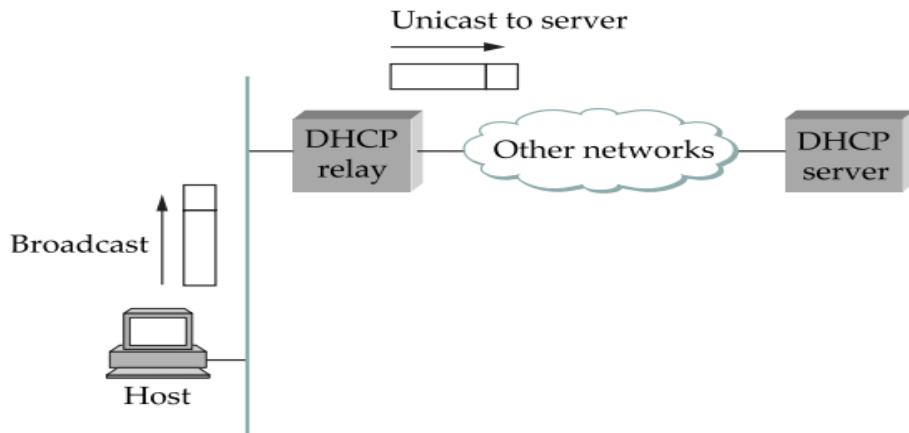
	that receives a broadcast ARP request will thereafter be able to determine the sender's address translation.	
<b>Uses</b>	The purpose of ARP involves finding the machine address of the other host.	It is utilized with minimum resources.

**Table 3.3 – ARP Vs RARP****Fig 3.26 – ARP & RARP****12. Discuss in detail about the concepts of DHCP.( April/may 2024)****Dynamic Host Configuration Protocol (DHCP)**

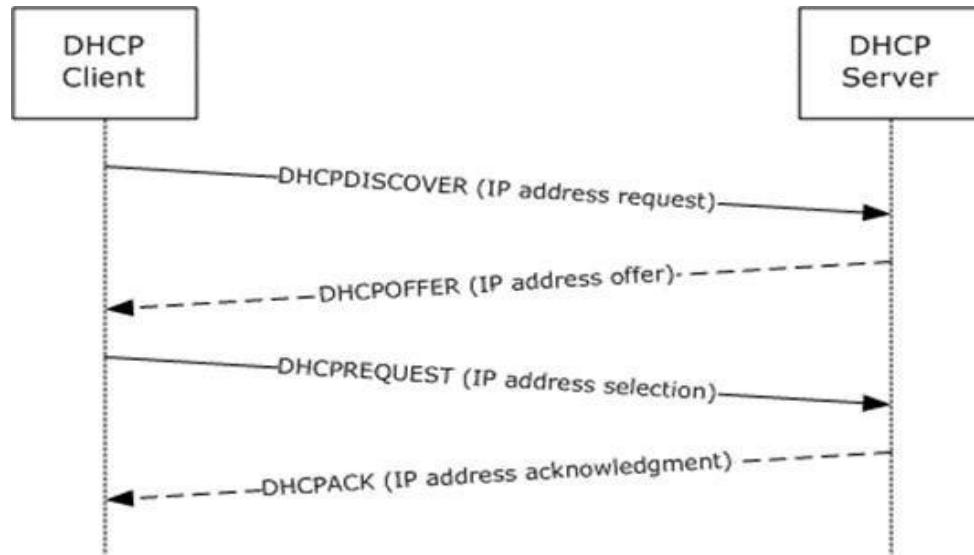
- The dynamic host configuration protocol is used to simplify the installation and maintenance of networked computers.
- DHCP is derived from an earlier protocol called BOOTP.
- Ethernet addresses are configured into network by manufacturer and they are unique.
- IP addresses must be unique on a given internetwork but also must reflect the structure of the internetwork.
- Most host Operating Systems provide a way to manually configure the IP information for the host.

**Drawbacks of manual configuration :**

1. A lot of work to configure all the hosts in a large network.
  2. Configuration process is error-prone.
- It is necessary to ensure that every host gets the correct network number and that no two hosts receive the same IP address.
  - For these reasons, automated configuration methods are required.
  - The primary method uses a protocol known as the Dynamic Host Configuration Protocol (DHCP).
  - The main goal of DHCP is to minimize the amount of manual configuration required for a host.
  - If a new computer is connected to a network, DHCP can provide it with all the necessary information for full system integration into the network.
  - DHCP is based on a client/server model.
  - DHCP clients send a request to a DHCP server to which the server responds with an IP address.
  - DHCP server is responsible for providing configuration information to hosts.
  - There is at least one DHCP server for an administrative domain.
  - The DHCP server can function just as a centralized repository for host configuration information.
  - The DHCP server maintains a pool of available addresses that it hands out to hosts on demand. (Refer fig 3.27)

**Fig 3.27 – DHCP**

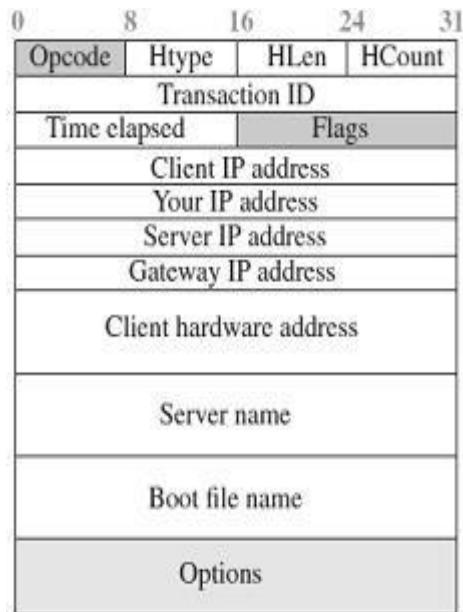
- A newly booted or attached host sends a DHCPDISCOVER message to a special IP address (255.255.255.255., which is an IP broadcast address).
- This means it will be received by all hosts and routers on that network.
- DHCP uses the concept of a relay agent. There is at least one relay agent on each network.
- DHCP relay agent is configured with the IP address of the DHCP server.
- When a relay agent receives a DHCPDISCOVER message, it unicasts it to the DHCP server and awaits the response, which it will then send back to the requesting client. (Refer fig 3.28).



**Fig 3.28 – DHCP Process flow**

#### **DHCP Message Format**

- A DHCP packet is actually sent using a protocol called the User Datagram Protocol (UDP). (Refer fig 3.29)



Opcode: Operation code, request (1) or reply (2)

Htype: Hardware type (Ethernet, ...)

HLen: Length of hardware address

HCount: Maximum number of hops the packet can travel

Transaction ID: An integer set by the client and repeated by the server

Time elapsed: The number of seconds since the client started to boot

Flags: First bit defines unicast (0) or multicast (1); other 15 bits not used

Client IP address: Set to 0 if the client does not know it

Your IP address: The client IP address sent by the server

Server IP address: A broadcast IP address if client does not know it

Gateway IP address: The address of default router

Server name: A 64-byte domain name of the server

Boot file name: A 128-byte file name holding extra information

Options: A 64-byte field with dual purpose described in text

**Fig 3.29 – DHCP Frame format**

**13. Write the difference between IPv4 & IPv6****Table 3.4 – IPv4 VS IPv6**

Property	IPv4	IPv6
Address size and network size	32 bits, network size 8-30 bits	128 bits, network size 64 bits
Packet header size	20-60 bytes	40 bytes
Header-level extension	limited number of small IP options	unlimited number of IPv6 extension headers
Fragmentation	sender or any intermediate router allowed to fragment	only sender may fragment
Control protocols	mixture of non-IP (ARP), ICMP, and other protocols	all control protocols based on ICMPv6
Minimum allowed MTU	576 bytes	1280 bytes
Path MTU discovery	optional, not widely used	strongly recommended
Address assignment	usually one address per host	usually multiple addresses per interface
Address types	use of unicast, multicast, and broadcast address types	broadcast addressing no longer used, use of unicast, multicast and anycast address types
Address configuration	devices configured manually or with host configuration protocols like DHCP	devices configure themselves independently using stateless address autoconfiguration (SLAAC) or use DHCP

**14. Discuss in detail about classful and classless IP addressing?(April/may2024)****Classful vs Classless Addressing**

- Classful and Classless addressing are methods used in networking to manage IP addresses. Classful addressing divides IP addresses into fixed classes (A, B, C, D, E), each with predefined ranges.
- In contrast, classless addressing, also known as **CIDR** (Classless Inter-Domain Routing), offers more flexibility by allowing addresses to be subdivided into smaller blocks called subnets. This flexibility helps optimize address allocation and supports the growth of the internet by efficiently managing IP address resources. We will see differences between classful and classless addressing in detail.

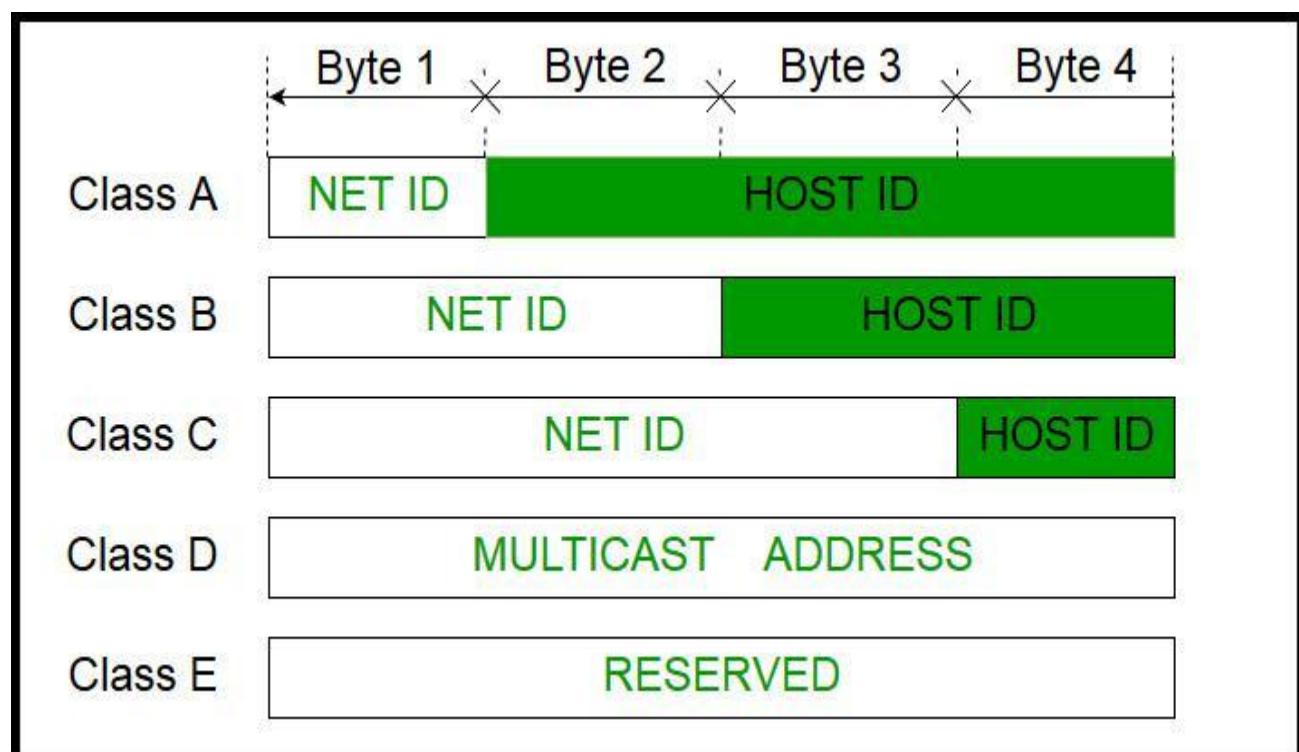
### Classful Addressing

Classful addressing was introduced in 1981, with classful routing, IPv4 addresses were divided into 5 classes(A to E), each with a predetermined range. The class of an IP address determines the network portion and the host portion based on its class-specific subnet mask. Classful addressing was inflexible and led to inefficiencies in address allocation, which prompted the development of **classless addressing (CIDR)** for more efficient use of IP address space.

Classes A-C: unicast addresses

Class D: multicast addresses

Class E: reserved for future use



### Classful Addressing

**Class A**

- In a class A address, the first bit of the first octet is always '0'. Thus, class A addresses range from 0.0.0.0 to 127.255.255.255(as 01111111 in binary converts to 127 in decimal).
- The first 8 bits or the first octet denote the network portion and the rest 24 bits or the 3 octets belong to the host portion. Its Subnet mask is 255.0.0.0.

**Example:** 10.1.1.1

**Exception -**

**-127.X.X.X is reserved for loopback**

**- 0.X.X.X is reserved for default network**

- Therefore, the actual range of class A addresses is: 1.0.0.0 to 126.255.255.255

**Class B**

- In a class B address, the first octet would always start with '10'. Thus, class B addresses range from 128.0.0.0 to 191.255.255.255.
- The first 16 bits or the first two octets denote the network portion and the remaining 16 bits or two octets belong to the host portion. Its Subnet mask is 255.255.0.0.

**Example: 172.16.1.1**

**Class C**

- In a class C address, the first octet would always start with '110'. Thus, class C addresses range from 192.0.0.0 to 223.255.255.255.
- The first 24 bits or the first three octets denote the network portion and the rest 8 bits or the remaining one octet belong to the host portion. Its Subnet mask is 255.255.255.0.

**Example:** 192.168.1.1

**Class D**

- Class D is used for multicast addressing and in a class D address the first octet would always start with '1110'. Thus, class D addresses range from 224.0.0.0 to 239.255.255.255. Its Subnet mask is not defined.

**Example:** 239.2.2.2

**Class D**

- addresses are used by routing protocols like OSPF, RIP, etc.

**Class E**

Class E addresses are reserved for research purposes and future use. The first octet in a class E address starts with '1111'. Thus, class E addresses range from 240.0.0.0 to 255.255.255.255. Its Subnet mask is not defined.

- Class A with a mask of 255.0.0.0 can support 128 Network, 16,777,216 addresses per network and a total of 2,147,483,648 addresses.
- Class B with a mask of 255.255.0.0 can support 16,384 Network, 65,536 addresses per network and a total of 1,073,741,824 addresses.
- Class C with a mask of 255.255.255.0 can support 2,097,152 Network, 256 addresses per network and a total of 536,870,912 addresses.

**someone requires 2000 addresses**

One way to address this situation would be to provide the person with class B network. But that would result in a waste of so many addresses.

Another possible way is to provide multiple class C networks, but that too can cause a problem as there would be too many networks to handle.

To resolve problems like the one mentioned above CIDR was introduced.

**Classless Addressing:**

**Classless Addressing** or **Classless Inter-Domain Routing** was introduced in 1993 to replace classful addressing. Classless Inter-Domain Routing (**CIDR**) is a method for efficiently allocating IP addresses and routing Internet Protocol (IP) packets. Unlike classful addressing, which divides IP addresses into fixed classes (A, B, C, etc.), CIDR allows for variable-length subnet masks (VLSM).

This means that networks can be divided into smaller, more flexible subnets according to their specific needs, rather than being constrained by predefined class boundaries.

**CIDR Notation:**

In CIDR subnet masks are denoted by /X. For example a subnet of 255.255.255.0 would be denoted by /24. To work a subnet mask in CIDR, we have to first convert each octet into its respective binary value. For example, if the subnet is of 255.255.255.0. then :

**First Octet**

255 has 8 binary 1's when converted to binary

**Second Octet**

255 has 8 binary 1's when converted to binary

**Third Octet**

255 has 8 binary 1's when converted to binary

**Fourth Octet**

*0 has 0 binary 1's when converted to binary*

Therefore, in total there are 24 binary 1's, so the subnet mask is /24. While creating a network in CIDR, a person has to make sure that the masks are contiguous, i.e. a subnet mask like 10111111.X.X.X can't exist. With CIDR, we can create Variable Length Subnet Masks, leading to less wastage of IP addresses. It is not necessary that the divider between the network and the host portions is at an octet boundary. For example, in CIDR a subnet mask like 255.224.0.0 or 11111111.11100000.00000000.00000000 can exist.



# MAILAM Engineering College

(Approved by AICTE, New Delhi, Affiliated to Anna University Chennai, Accredited by NBA, TCS & NAAC - 'A' Grade)

## DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND DATA SCIENCE

**II YEAR / IV SEM**

### **CS3591 – COMPUTER NETWORKS**

#### **UNIT IV – ROUTING**

#### **SYLLABUS:**

Routing and protocols: Unicast routing - Distance Vector Routing - RIP - Link State Routing – OSPF – Path-vector routing - BGP - Multicast Routing: DVMRP – PIM.

#### **PART A**

#### **1. List the various routing algorithms.**

##### **UNICAST ROUTING ALGORITHMS**

- Distance Vector Routing Algorithm – Routing Information Protocol (RIP)
- Link State Routing Algorithm – Open Shortest Path First Protocol (OSPF)
- Path-Vector Routing Algorithm - Border Gateway Protocol (BGP)

##### **MULTICAST ROUTING ALGORITHMS**

- DVMRP - Distance Vector Multicast Routing Protocol
- PIM – Protocol Independent Multicast

#### **2. Define Bellman-Ford Equation.**

- This equation is used to find the least cost (shortest distance) between a source node,  $x$ , and a destination node,  $y$ , through some intermediary nodes ( $a, b, c, \dots$ ).
- The following shows the general case in which  $D_{ij}$  is the shortest distance and  $c_{ij}$  is the cost between nodes  $i$  and  $j$ .

$$D_{xy} = \min \{ (c_{xa} + D_{ay}), (c_{xb} + D_{by}), (c_{xc} + D_{cy}), \dots \}$$

- In distance-vector routing, normally we want to update an existing least cost with a least cost through an intermediary node, such as **z**, if the latter is shorter.

$$D_{xy} = \min \{ D_{xy}, (c_{xz} + D_{zy}) \}$$

### **3. Define Border Gateway Protocol (BGP).**

- The Border Gateway Protocol version 4 (BGP4) is the only interdomain routing protocol, based on the path-vector algorithm.
- BGP allows routers to carry specific policies or constraints that they must meet.
- In BGP, two contributing (casual) routers can exchange routing information even if they are located in two different autonomous systems.

### **4. Write the keys for understanding the distance vector routing.**

The three keys for understanding the algorithm are,

- Knowledge about the whole networks
- Routing only to neighbors
- Information sharing at regular intervals

### **5. Write the keys for understanding the link state routing.**

The three keys for understanding the algorithm are,

- Knowledge about the neighborhood.
- Routing to all neighbors.
- Information sharing when there is a range.

### **6. How the packet cost referred in distance vector and link state routing?**

- In distance vector routing, cost refer to hop count while in case of link state routing, cost is a weighted value based on a variety of factors such as security levels, traffic or the state of the link.

### **7. What are the features in OSPF?**

- Authentication of routing messages.
- Additional hierarchy.
- Load balancing.

**8. What are the different routing techniques available to manage routing table entries?**

1. Next hop routing.
2. Network specific routing
3. Host specific routing
4. Default routing

**9. What are the main disadvantages of distance vector routing?**

1. Split horizon
2. Count to infinity problem

**10. What are the desirable properties of routing algorithms?**

1. Correctness
2. Simplicity
3. Robustness
4. Stability
5. Fairness
6. Optimality

**11. Give the types of routing table.**

- There are two types of routing table. They are, **Static routing table:** The entries are created or update manually by an administrator.
- **Dynamic routing table:** The entries are updated automatically by dynamic routing protocols such as RIP, OSPF or BGP.

**12. Define routing protocol.**

Routing protocols is defined as “a combination of rules and procedures, which allows routers to share whatever they know about the internet or their neighborhood. It also includes procedures for combining information received from other routers”.

**13. Mention the types (classes) of routing protocol.**

There are two basic categories of routing. They are,

- Intradomain routing, and
- Interdomain routing

**14. Distinguish between Intradomain and Interdomain routing protocol.**

S.No	Intradomain Routing	Interdomain Routing
1.	It is defined as routing inside an AS.	It is defined as routing between AS.
2.	It is classified as, 1.Distance Vector, 2.Link State	The path vector is of type interdomain.
3.	RIP (Routing Information Protocol) Is an implementation of the distance vector protocol and OSPF(Open shortest first) is an implementation of link state protocol.	BGP (Border Gateway Protocol) is an implementation of the path vector protocol.

**15. Define AS.**

A group of networks and routers under the authority of single administration is called as Autonomous System (AS).

**16. Define RIP (or) Express the purpose of RIP.**

Routing information protocol (RIP) is a simple protocol intradomain routing protocol used inside and Autonomous System(AS) based distance vector routing algorithm, in which each router shares, at regular intervals, its knowledge about the entire AS with its neighbors.

**17. Mention the advantages of RIP over OSPF.**

(i)RIP for IP is easy to implement. In its simplest default configuration, RIP for IP is as easy as configuring IP addresses and subnet masks for each router interface and then turning on the router.

(ii)RIP for IP has a large installed base consisting of small and medium-sized IP internetworks that do not wish to bear the design and configuration burden of OSPF.

**18. What is Link state routing (LSR)?**

It is a lowest-cost algorithm used in routing. The information on directly connected neighbors and current link costs are flooded to all routers; each router uses this information to build a view of the network which is the base to make forwarding decisions.

**19. What do you meant by flooding?**

Flooding means that a router sends all its link-state information about its neighbors, then the neighbors forward this information to their neighbors and so on. Thereby, every router receives the copy of the same information. This process continues until the information has reached all the nodes in the network.

**20. Elaborate OSPF.**

Open shortest path first (OSPF) is protocol widely used for intra-AS routing in the internet. It is the popular intradomain routing protocol based on link state routing that uses flooding of link-state information and a Dijkstra least-cost path algorithm.

**21. Mention the advantages of OSPF.**

OSPF has the following advantages

- (i) Authentication
- (ii) Support for hierarchy within a single routing domain
- (iii) Multiple same-cost paths and
- (iv) Integrated support for unicast and multicast routing.

**22. Compare distance vector routing with link state routing.**

S.No	<b>Distance vector routing(DVR)</b>	<b>Link state routing(LSR)</b>
1.	In DVR, each router periodically shares its knowledge about the entire network with its neighbours.	In LSR, each router shares its knowledge of its neighbourhood with all routers in the internetwork.
2.	The three important keys are, ->Knowledge about the whole network. ->Routing only to neighbours ->Information sharing at regular intervals.	The three important keys are, ->Knowledge about the neighbourhood. ->Routing to all routers ->Information sharing when there is a change.

**23. Define an area.**

The link-state routing protocols such as OSPF and IS-IS can be used to partition a routing domain(AS) into subdomains called areas, to improve scalability, which is a set of adjacent routers that administratively configured to exchange full routing information with each other.

**24. Define BGP.**

The Border Gateway Protocol(BGP) is an interdomain routing protocol based on path vector routing by which different autonomous system (ASs) exchange reachability information.

**25. Mention the names of two interdomain routing protocols.**

There have been two major interdomain routing protocols in the history of the Internet.

- (i) Exterior Gateway Protocol (EGP) and
- (ii) Border Gateway Protocol(BGP).

**26. What is EGP? Mention its drawbacks.**

- Exterior gateway protocol (EGP) is an interdomain routing protocol of the internet, which was used by exterior gateway (routers) of autonomous systems to exchange routing information with other autonomous systems, which had a number of limitations.
- EGP was designed when the Internet had a treelike topology, and did not allow for the topology to become more general and autonomous systems are connected only as parents and children and not as peers. The replacement for EGP is the Border Gateway Protocol (BGP).

**27. Define an IGP.**

Interior Gateway Protocol(IGP) is a routing protocol used to exchange routing information among routers within a single autonomous system.

**28. Write the functions of BGP.**

BGP provides each AS:

- (i) Obtain subnet reachability information from neighboring ASs.
- (ii) Propagate the reachability information to all routers internal to the AS.
- (iii) Determine “good” routes to subnets based on the reachability information and on AS policy.

**29. What is multicast?**

Multicast is a special form of broadcast in which a single source transmits the packets and they are delivered to specified subgroup of network hosts(one-to-many).

**30. Give the comparison of unicast, multicast and broadcast Routing.(April/may 2024)**

S.No	<b>Unicasting</b>	<b>Multicasting</b>	<b>Broadcasting</b>
1.	One source and one destination	One source and a group of destinations.	One source and all destinations.
2.	Relationship is one-to-one	Relationship is one-to-many	Relationship is one-to-all
3.	Both source and destination addresses are unicast addresses	The source address is unicast address, but the destination address is a group address	Both source and destination addresses are broadcast addresses
4	In unicasting, the router forwards the received packet through only one of its interface	In multicasting, the router forwards the received packet through several of its interfaces.	In broadcasting, the router forwards the received packet through all its interfaces.

**31. Expand DVMRP.**

Distance Vector Multicast Routing Protocol (DVMRP) is a multicast distance vector routing uses the source-based least cost trees, but the router never actually makes a routing table.

**32. Name the strategies used in multicast DVR protocol.**

The multicast DVR algorithm uses a process based on four decision-making strategies. Each strategy is built on its predecessor.

- (i) Flooding,
- (ii) Reverse Path Forwarding(RPF),
- (iii) Reverse Path Broadcasting(RPB), and
- (iv) Reverse Path Multicasting(RPM)

**33. What do you meant by PIM?**

- Protocol independent multicast (PIM) is a multicasting protocol family with two independent multicast routing protocols such as:
  - (i) PIM-DM (Dense Mode) and
  - (ii) PIM-SM (Spare Mode)
- Both protocols are unicast-protocol dependent.

**34. Define the terms PIM-DM & PIM-SM.**

- Protocol independent multicast- Dense Mode (PIM-DM) is used in a dense multicast environment, such as a LAN. It is a source-based tree routing protocol that uses RPF and pruning and grafting strategies for multicasting .
- Protocol independent multicasting-Spare Mode (PIM-SM).
- Is used in a spares multicast environment such as a WAN. PIM-SM is group-shared tree routing protocol that has a rendezvous point (RP) as the source of the tree. PIM-SM is similar to CBT but uses a simpler procedure.

**35. Write any two difference between Connection oriented and Connectionless service?(April/may 2023)**

<b>Connection-oriented Service</b>	<b>Connection-less Service</b>
Connection-oriented service is related to the telephone system.	Connection-less service is related to the postal system.
Connection-oriented service is preferred by long and steady communication.	Connection-less Service is preferred by bursty communication.
Connection-oriented Service is necessary.	Connection-less Service is not compulsory.
Connection-oriented Service is feasible.	Connection-less Service is not feasible.
In connection-oriented Service, Congestion is not possible.	In connection-less Service, Congestion is possible.

**36.List the Multicast Routing Protocols?(april/may 2023)**

- Protocol Independent Multicast (**PIM**)
- Distance Vector Multicast Routing Protocol (**DVMRP**)
- Multicast Open Shortest Path First (**MOSPF**)

**37.What are the important attributes of good routing algorithm?(Nov/dec 2023)**

- Priority and order — Select the routing priority for each task, such as a First In First Out (FIFO) or Last In First Out (LIFO) algorithm.
- Time of day routing — Redefined attributes allow you to route tasks based on time of day or day of the week.

**PART B****1. Discuss the concepts of Unicast Routing.****Synopsis:**

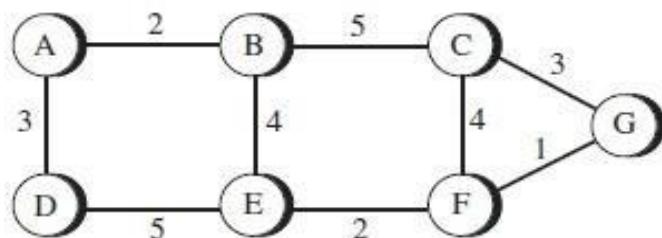
- **Introduction**
- **Network as a graph**

**Introduction:**

- Routing is the process of selecting best paths in a network.
- In unicast routing, a packet is routed, hop by hop, from its source to its destination by the help of forwarding tables.
- Routing a packet from its source to its destination means routing the packet from a *source router* (the default router of the source host) to a *destination router* (the router connected to the destination network).
- The source host needs no forwarding table because it delivers its packet to the default router in its local network.
- The destination host needs no forwarding table either because it receives the packet from its default router in its local network.
- Only the intermediate routers in the networks need forwarding tables.

**NETWORK AS A GRAPH**

- The Figure below shows a graph representing a network.

**Fig 4.1 – Unicast routing example network**

- The nodes of the graph, labeled A through G, may be hosts, switches, routers, or networks.

- The edges of the graph correspond to the network links. (**Refer Fig 4.1**)
- Each edge has an associated cost.
- The basic problem of routing is to find the lowest-cost path between any two nodes, where the cost of a path equals the sum of the costs of all the edges that make up the path.
- This static approach has several problems:
  - ❖ It does not deal with node or link failures.
  - ❖ It does not consider the addition of new nodes or links.
  - ❖ It implies that edge costs cannot change.
- For these reasons, routing is achieved by running routing protocols among the nodes.
- These protocols provide a distributed, dynamic way to solve the problem of finding the lowest-cost path in the presence of link and node failures and changing edge costs.

**2. Write short notes on autonomous systems (AS) in routing protocols with inter domain and intra domain.**

**Synopsis:**

- **Introduction**
- **Internet structure**
- **Inter domain routing**
- **Traffic on the internet is of two types**
- **Autonomous systems (as) are classified as**
- **Policies used by autonomous systems**
- **Challenges in inter-domain routing protocol**
- **Types of routing protocols**

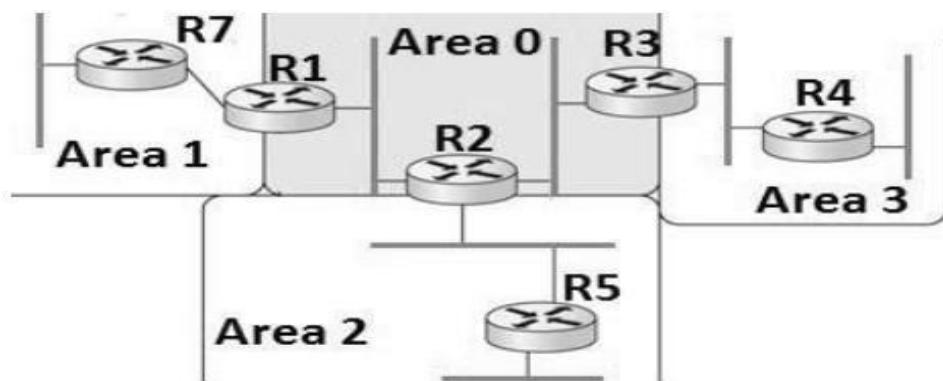
**Introduction:**

- A protocol is more than an algorithm.
- A protocol needs to define its domain of operation, the messages exchanged, communication between routers, and interaction with protocols in other domains.
- A routing protocol specifies how routers communicate with each other, distributing information that enables them to select routes between any two nodes on a computer network.

- Routers perform the "traffic directing" functions on the Internet; data packets are forwarded through the networks of the internet from router to router until they reach their destination computer.
- Routing algorithms determine the specific choice of route.
- Each router has a prior knowledge only of networks attached to it directly.
- A routing protocol shares this information first among immediate neighbors, and then throughout the network. This way, routers gain knowledge of the topology of the network.
- The ability of routing protocols to dynamically adjust to changing conditions such as disabled data lines and computers and route data around obstructions is what gives the Internet its survivability and reliability.
- The specific characteristics of routing protocols include the manner in which they avoid routing loops, the manner in which they select preferred routes, using information about hop costs, the time they require to reach routing convergence, their scalability, and other factors.

### INTERNET STRUCTURE

- Internet has a million networks. Routing table entries per router should be minimized.
- Link state routing protocol is used to partition domain into areas.
- An routing area is a set of routers configured to exchange link-state information.
- Area introduces an additional level of hierarchy.
- Thus domains can grow without burdening routing protocols.



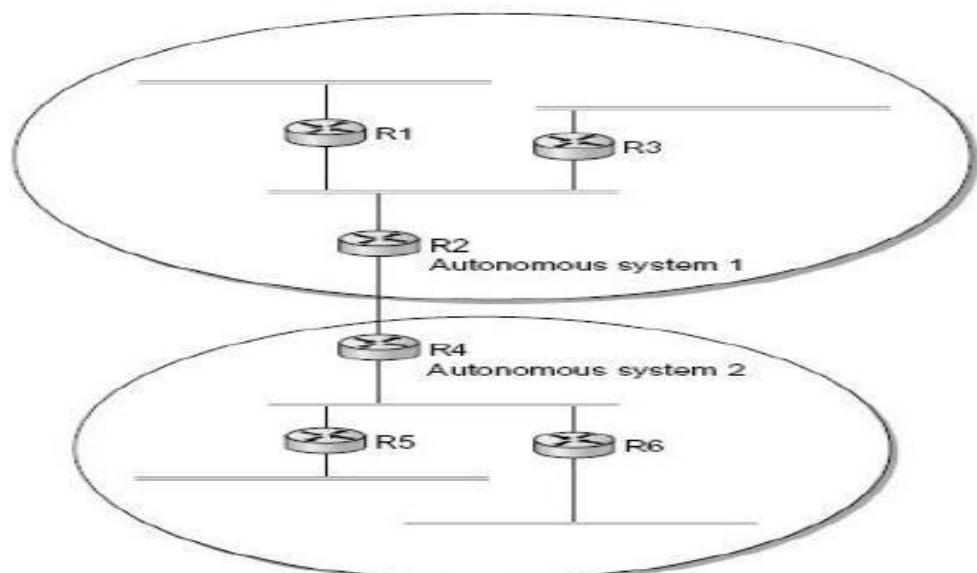
**Fig 4.2 – Internet structure**

- There is one special area—the backbone area, also known as area 0.
- Routers R1, R2 and R3 are part of backbone area. (**Refer Fig 4.2**)

- Routers in backbone area are also part of non-backbone areas. Such routers are known as Area Border Routers (ABR).
- Link-state advertisement is exchanged amongst routers in a non-backbone area.
- They do not see LSAs of other areas. For example, area 1 routers are not aware of area 3 routers.
- ABR advertises routing information in their area to other ABRs.
- For example, R2 advertises area 2 routing information to R1 and R3, which in turn pass onto their areas.
- All routers learn how to reach all networks in the domain.
- When a packet is to be sent to a network in another area, it goes through backbone area via ABR and reaches the destination area.
- Routing Areas improve scalability but packets may not travel on the shortest path.

### INTER DOMAIN ROUTING

- Internet is organized as autonomous systems (AS) each of which is under the control of a single administrative entity.
- A corporation's complex internal network might be a single AS, as may the network of a single Internet Service Provider (ISP). (**Refer Fig 4.3**)
- Interdomain routing shares reachability information between autonomous systems.

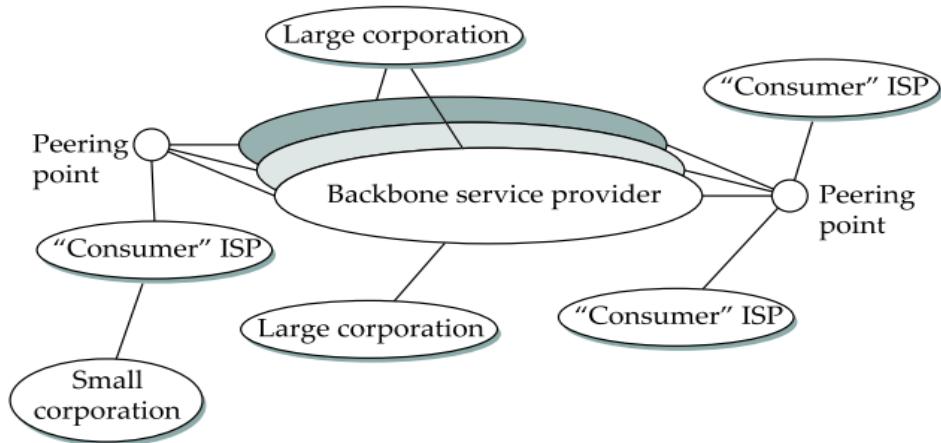


**Fig 4.3 – Inter domain routing**

- The basic idea behind autonomous systems is to provide an additional way to

hierarchically aggregate routing information in a large internet, thus improving scalability.

- Internet has backbone networks and sites. Providers connect at a peering point.  
**(Refer Fig 4.4)**



**Fig 4.4 – Backbone service provider**

#### Traffic on the internet is of two types:

- Local Traffic - Traffic within an autonomous system is called local.
- Transit Traffic - Traffic that passes through an autonomous system is called transit.

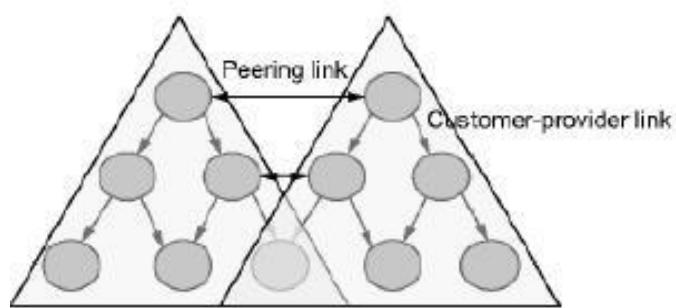
#### Autonomous Systems (AS) are classified as:

- Stub AS - is connected to only one another autonomous system and carries local traffic only (e.g. Small corporation).
- Multihomed AS - has connections to multiple autonomous systems but refuses to carry transit traffic (e.g. Large corporation).
- Transit AS - has connections to multiple autonomous systems and is designed to carry transit traffic (e.g. Backbone service provider).

#### Policies Used By Autonomous Systems :

- Provider-Customer—Provider advertises the routes it knows, to the customer and advertises the routes learnt from customer to everyone.
- Customer-Provider—Customers want the routes to be diverted to them. So they advertise their own prefixes and routes learned from customers to provider and advertise routes learned from provider to customers.

- Peer—Two providers access to each other's customers without having to pay.  
**(Refer Fig 4.5)**

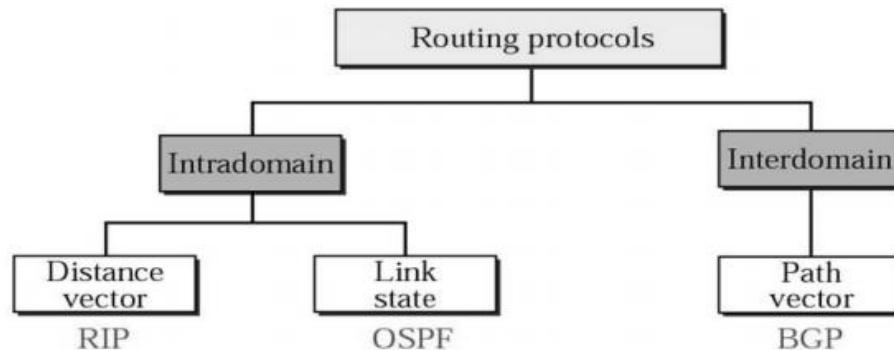


**Fig 4.5 – Peering link in AS**

### CHALLENGES IN INTER-DOMAIN ROUTING PROTOCOL

- Each autonomous system has an intra-domain routing protocol, its own policy and metric.
- Internet backbone must be able to route packets to the destination that complies with policies of autonomous system along a loopless path.
- Service providers have trust deficit and may not trust advertisements by other AS, or may refuse to carry traffic from other AS.

### TYPES OF ROUTING PROTOCOLS (Refer Fig 4.6)



**Fig 4.6 – Routing protocol types**

- Two types of Routing Protocols are used in the Internet:

**Intradomain routing**

- Routing within a single autonomous system.
- Routing Information Protocol (RIP) - based on the distance-vector algorithm - (REFER distance-vector routing algorithm).
- Open Shortest Path First (OSPF) - based on the link-state algorithm - (REFER link-state routing algorithm).

**Interdomain routing**

- Routing between autonomous systems.
- Border Gateway Protocol (BGP) - based on the path-vector algorithm - (REFER Path Vector routing algorithm).

**3. List the unicast routing algorithms and explain the concepts of distance vector routing (DSR), Routing information protocol (RIP), Bellman- Ford algorithm (Intra domain routing protocol).**

**Synopsis:**

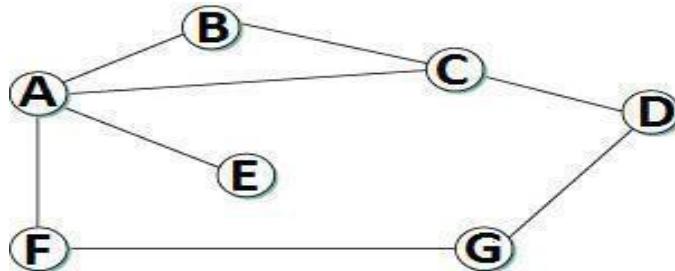
- **Introduction**
  - **Updation of Routing Tables**
  - **Periodic Update**
  - **Triggered Update**
  - **Routing information protocol (rip)**

**Introduction:**

- Distance vector routing is distributed, i.e., algorithm is run on all nodes.
- Each node knows the distance (cost) to each of its directly connected neighbors.
- Nodes construct a vector (Destination, Cost, NextHop) and distributes to its neighbors.
- Nodes compute routing table of minimum distance to every other node via

Next Hop using information obtained from its neighbors.

### Initial State



**Fig 4.7 – Example network – Initial state**

- In given network, cost of each link is 1 hop. (**Refer Fig 4.7**)
- Each node sets a distance of 1 (hop) to its immediate neighbor and cost to itself as 0.
- Distance for non-neighbors is marked as unreachable with value  $\infty$  (infinity).
- For node A, nodes B, C, E and F are reachable, whereas nodes D and G are unreachable. (**Refer Fig 4.8**)

Destination	Cost	NextHop
A	0	A
B	1	B
C	1	C
D	$\infty$	—
E	1	E
F	1	F
G	$\infty$	—

Destination	Cost	NextHop
A	1	A
B	1	B
C	0	C
D	1	D
E	$\infty$	—
F	$\infty$	—
G	$\infty$	—

Destination	Cost	NextHop
A	1	A
B	$\infty$	—
C	$\infty$	—
D	$\infty$	—
E	$\infty$	—
F	0	F
G	1	G

**Fig 4.8 – Routing table for separate node**

- The initial table for all the nodes is given below,

Initial Distances Stored at Each Node (Global View)							
Information Stored at Node	Distance to Reach Node						
	A	B	C	D	E	F	G
A	0	1	1	$\infty$	1	1	$\infty$
B	1	0	1	$\infty$	$\infty$	$\infty$	$\infty$
C	1	1	0	1	$\infty$	$\infty$	$\infty$
D	$\infty$	$\infty$	1	0	$\infty$	$\infty$	1
E	1	$\infty$	$\infty$	$\infty$	0	$\infty$	$\infty$
F	1	$\infty$	$\infty$	$\infty$	$\infty$	0	1
G	$\infty$	$\infty$	$\infty$	1	$\infty$	1	0

**Fig 4.9 – Initial routing table for all nodes.**

- Each node sends its initial table (distance vector) to neighbors and receives their estimate.
- Node A sends its table to nodes B, C, E & F and receives tables from nodes B, C, E & F. (**Refer Fig 4.9**)
- Each node updates its routing table by comparing with each of its neighbor's table
- For each destination, Total Cost is computed as:

- Total Cost = Cost (Node to Neighbor) + Cost (Neighbor to Destination)
- If Total Cost < Cost then
- Cost = Total Cost and NextHop = Neighbor
- Node A learns from C's table to reach node D and from F's table to reach node G.
- Total Cost to reach node D via C = Cost (A to C) + Cost(C to D); Cost = 1 + 1 = 2.
  - ✓ Since  $2 < \infty$ , entry for destination D in A's table is changed to (D, 2, C)
  - ✓ Total Cost to reach node G via F = Cost(A to F) + Cost(F to G) = 1 + 1 = 2
  - ✓ Since  $2 < \infty$ , entry for destination G in A's table is changed to (G, 2, F)
- Each node builds complete routing table after few exchanges amongst its neighbors.

*Node A's final routing table*

Destination	Cost	NextHop
A	0	A
B	1	B
C	1	C
D	2	C
E	1	E
F	1	F
G	2	F

**Fig 4.10 – Final routing table for node A**

- System stabilizes when all nodes have complete routing information, i.e., convergence. (**Refer Fig 4.10**)
- Routing tables are exchanged periodically or in case of triggered update.
- The final distances stored at each node is given below: (**Refer Fig 4.11**).

Final Distances Stored at Each Node (Global View)							
Information Stored at Node	Distance to Reach Node						
	A	B	C	D	E	F	G
A	0	1	1	2	1	1	2
B	1	0	1	2	2	2	3
C	1	1	0	1	2	2	2
D	2	2	1	0	3	2	1
E	1	2	2	3	0	2	3
F	1	2	2	2	2	0	1
G	2	3	2	1	3	1	0

**Fig 4.11 – Final routing table for all nodes****Updation of Routing Tables**

- There are two different circumstances under which a given node decides to send a routing update to its neighbors.

**Periodic Update**

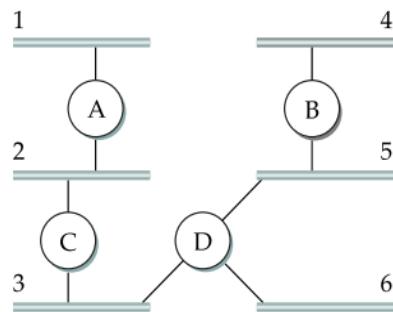
- In this case, each node automatically sends an update message every so often, even if nothing has changed.
- The frequency of these periodic updates varies from protocol to protocol, but it is typically on the order of several seconds to several minutes.

**Triggered Update**

- In this case, whenever a node notices a link failure or receives an update from one of its neighbors that causes it to change one of the routes in its routing table.
- Whenever a node's routing table changes, it sends an update to its neighbors, which may lead to a change in their tables, causing them to send an update to their neighbors.

**ROUTING INFORMATION PROTOCOL (RIP)**

- RIP is an intra-domain routing protocol based on distance-vector algorithm.

**Example****Fig 4.12 – Example network – RIP**

- Routers advertise the cost of reaching networks. Cost of reaching each link is 1 hop. For example, router C advertises to A that it can reach network 2, 3 at cost 0 (directly connected), networks 5, 6 at cost 1 and network 4 at cost 2. (**Refer Fig 4.12**)
- Each router updates cost and next hop for each network number.
- Infinity is defined as 16, i.e., any route cannot have more than 15 hops. Therefore RIP can be implemented on small-sized networks only.
- Advertisements are sent every 30 seconds or in case of triggered update.

0	7	15	31
command	version	must be zero	
address family identifier		must be zero	
	IP address		
	must be zero		
	must be zero		
	metric		

**Fig 4.13 – Frame format – RIP**

- **Command** - It indicates the packet type.
- **Value 1 represents a request packet. Value 2 represents a response packet.**
- **Version** - It indicates the RIP version number. For RIPv1, the value is 0x01.
- **Address Family Identifier** - When the value is 2, it represents the IP protocol.
- **IP Address** - It indicates the destination IP address of the route. It can be the addresses of only the natural network segment.
- **Metric** - It indicates the hop count of a route to its destination. (**Refer Fig 4.13**).

- 4. Explain Link state routing (LSR), Open shortest path first (OSPF), Dijkstra's algorithm concepts in detail (Intra domain routing protocol).**

**Synopsis:**

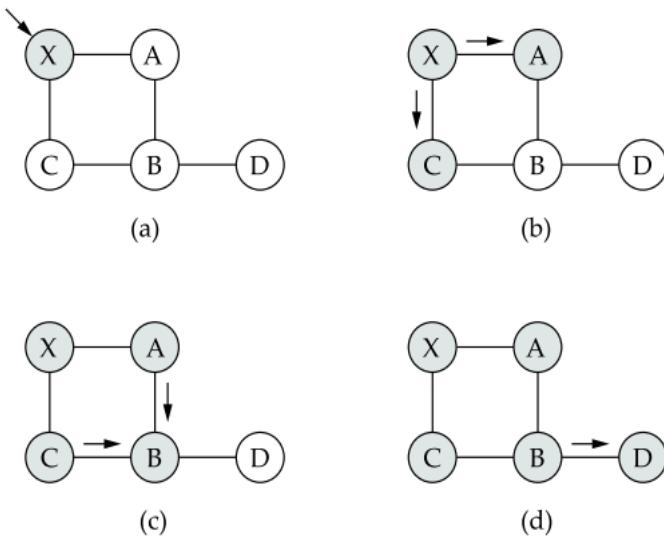
- **Introduction**
- **Reliable Flooding**
- **Route Calculation**
- **Dijkstra's shortest path algorithm (forward search algorithm)**
- **OPEN SHORTEST PATH FIRST PROTOCOL (OSPF)**
- **Link State Packet Format**
- **Difference Between Distance-Vector And Link-State Algorithms**

**Introduction:**

- Each node knows state of link to its neighbors and cost.
- Nodes create an update packet called link-state packet (LSP) that contains:
  - ID of the node
  - List of neighbors for that node and associated cost
  - 64-bit Sequence number
  - Time to live
- Link-State routing protocols rely on two mechanisms:
  - **Reliable flooding** of link-state information to all other nodes
  - **Route calculation** from the accumulated link-state knowledge.

**Reliable Flooding**

- Each node sends its LSP out on each of its directly connected links.
- When a node receives LSP of another node, checks if it has an LSP already for that node.
- If not, it stores and forwards the LSP on all other links except the incoming one.
- Else if the received LSP has a bigger sequence number, then it is stored and forwarded.
- Older LSP for that node is discarded.
- Otherwise discard the received LSP, since it is not latest for that node.



**Fig 4.14 – Flooding of link-state packets. (a) LSP arrives at node X; (b) X floods LSP to A and C; (c) A and C flood LSP to B (but not X); (d) flooding is complete.**

- Thus recent LSP of a node eventually reaches all nodes, i.e., reliable flooding.
- Flooding of LSP in a small network is as follows:
  - When node  $X$  receives  $Y$ 's LSP (fig a), it floods onto its neighbors  $A$  and  $C$  (fig b).
  - Nodes  $A$  and  $C$  forward it to  $B$ , but does not send it back to  $X$  (fig c).
  - Node  $B$  receives two copies of LSP with same sequence number.
  - Accepts one LSP and forwards it to  $D$  (fig d). Flooding is complete.
- LSP is generated either periodically or when there is a change in the topology.

**(Refer Fig 4.14)**

### Route Calculation

- Each node knows the entire topology, once it has LSP from every other node.
- Forward search algorithm is used to compute routing table from the received LSPs.
- Each node maintains two lists, namely Tentative and Confirmed with entries of the form (Destination, Cost, Next Hop).

### DIJKSTRA'S SHORTEST PATH ALGORITHM (FORWARD SEARCH ALGORITHM) (Nov/dec2023)

1. Each host maintains two lists, known as **Tentative** and **Confirmed**.
2. Initialize the Confirmed list with an entry for the Node (Cost = 0).
3. Node just added to Confirmed list is called Next. Its LSP is examined.

- 4.** For each neighbor of Next, calculate cost to reach each neighbor as Cost (Nodeto Next) + Cost (Next to Neighbor).
- If Neighbor is neither in Confirmed nor in Tentative list, then add (Neighbor, Cost, NextHop) to Tentative list.
  - If Neighbor is in Tentative list, and Cost is less than existing cost, then replace the entry with (Neighbor, Cost, NextHop).
2. If Tentative list is empty then Stop, otherwise move least cost entry from Tentative list to Confirmed list. Go to Step 2. (**Refer Fig 4.15**)

**Example :**

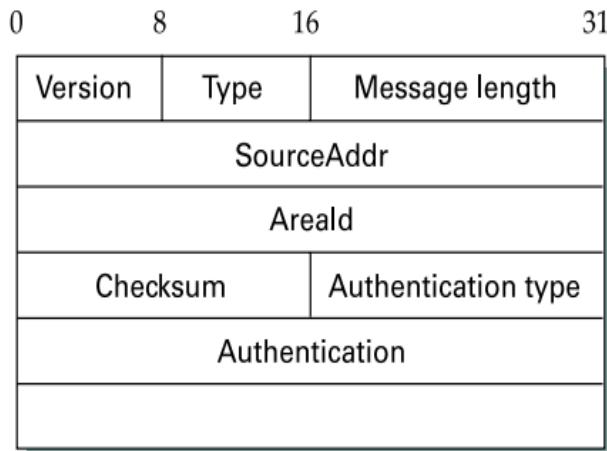
Step	Confirmed	Tentative	Comments
1	(D,0,-)		Since D is the only new member of the confirmed list, look at its LSP.
2	(D,0,-)	(B,11,B) (C,2,C)	D's LSP says we can reach B through B at cost 11, which is better than anything else on either list, so put it on Tentative list; same for C.
3	(D,0,-) (C,2,C)	(B,11,B)	Put lowest-cost member of Tentative (C) onto Confirmed list. Next, examine LSP of newly confirmed member (C).
4	(D,0,-) (C,2,C)	(B,5,C) (A,12,C)	Cost to reach B through C is 5, so replace (B,11,B). C's LSP tells us that we can reach A at cost 12.
5	(D,0,-) (C,2,C) (B,5,C)	(A,12,C)	Move lowest-cost member of Tentative (B) to Confirmed, then look at its LSP.
6	(D,0,-) (C,2,C) (B,5,C)	(A,10,C)	Since we can reach A at cost 5 through B, replace the Tentative entry.
7	(D,0,-) (C,2,C) (B,5,C) (A,10,C)		Move lowest-cost member of Tentative (A) to Confirmed, and we are all done.

**Fig 4.15 – OSPF**

### OPEN SHORTEST PATH FIRST PROTOCOL (OSPF)

- OSPF is a non-proprietary widely used link-state routing protocol.
- OSPF Features are:
  - **Authentication**—Malicious host can collapse a network by advertising to reach every host with cost 0. Such disasters are averted by authenticating routing updates.
  - **Additional hierarchy**—Domain is partitioned into areas, i.e., OSPF is more scalable.
  - **Load balancing**—Multiple routes to the same place are assigned same cost. Thus traffic is distributed evenly.

### Link State Packet Format



**Fig 4.16 – Packet format**

**Version** – represents the current version, i.e., 2. (**Refer Fig 4.16**)

**Type** – represents the type (1–5) of OSPF message.

Type 1 - “hello” message, Type 2 - request, Type 3 – send ,

Type 4 –acknowledge the receipt of link state messages ,

Type 5 - reserved

**SourceAddr** – identifies the sender

**AreaId** – 32-bit identifier of the area in which the node is located

**Checksum** – 16-bit internet checksum

**Authentication type** – 1 (simple password), 2 (cryptographic authentication).

**Authentication** – contains password or cryptographic checksum.

### Difference Between Distance-Vector And Link-State Algorithms

<b>Distance vector Routing</b>	<b>Link state Routing</b>
Each node talks only to its directly connected neighbors, but it tells them everything it has learned (i.e., distance to all nodes).	Each node talks to all other nodes, but it tells them only what it knows for sure (i.e., only the state of its directly connected links).

**5. Explain Path vector routing (PVR), Boarder gateway protocol (BGP) concepts in detail (Inter domain routing protocol). (April/may 2024)**

**Synopsis:**

- **Introduction**
- **Spanning Trees**
  - ✓ Example
- **Path Vectors made at booting time**
- **Updating Path Vectors**
- **Border Gateway Protocol (BGP)**
- **iBGP - interior BGP**

### **Introduction**

- Path-vector routing is an asynchronous and distributed routing algorithm.
- The Path-vector routing is not based on least-cost routing.
- The best route is determined by the source using the policy it imposes on the route.
- In other words, the source can control the path.
- Path-vector routing is not actually used in an internet, and is mostly designed to route a packet between ISPs.

### **Spanning Trees**

- In path-vector routing, the path from a source to all destinations is determined by the best spanning tree.
- The best spanning tree is not the least-cost tree.
- It is the tree determined by the source when it imposes its own policy.
- If there is more than one route to a destination, the source can choose the route that meets its policy best.
- A source may apply several policies at the same time.
- One of the common policies uses the minimum number of nodes to be visited. Another common policy is to avoid some nodes as the middle node in a route.
- The spanning trees are made, gradually and asynchronously, by each node. When a node is booted, it creates a path vector based on the information it can obtain about its immediate neighbor.
- A node sends greeting messages to its immediate neighbors to collect these pieces of information.

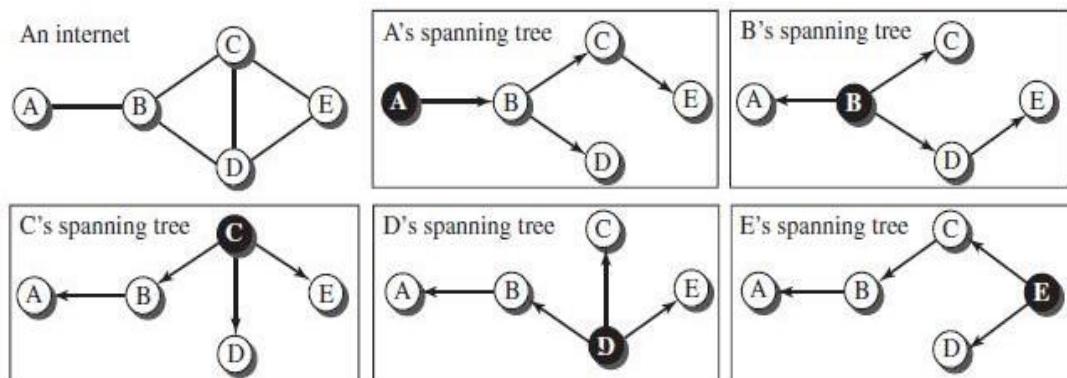
- Each node, after the creation of the initial path vector, sends it to all its immediate neighbors.
- Each node, when it receives a path vector from a neighbor, updates its path vector using the formula,

$$\text{Path}(x, y) = \text{best} \{ \text{Path}(x, y), [(x + \text{Path}(v, y))] \} \quad \text{for all } v's \text{ in the internet.}$$

- The policy is defined by selecting the best of multiple paths.
- Path-vector routing also imposes one more condition on this equation.
- If Path (v, y) includes x, that path is discarded to avoid a loop in the path.
- In other words, x does not want to visit itself when it selects a path to y.

**Example:**

- The **Figure 4.17** below shows a small internet with only five nodes.
- Each source has created its own spanning tree that meets its policy.
- The policy imposed by all sources is to use the minimum number of nodes to reach a destination.
- The spanning tree selected by A and E is such that the communication does not pass through D as a middle node.
- Similarly, the spanning tree selected by B is such that the communication does not pass through C as a middle node.

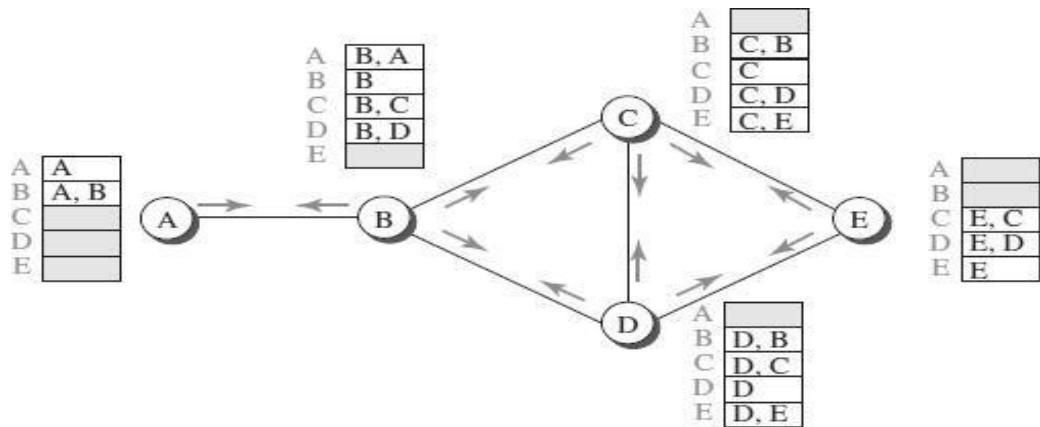


**Fig 4.17 – Spanning Tree**

**Path Vectors made at booting time**

- The **Figure 4.18** below shows all of these path vectors for the example.
- Not all of these tables are created simultaneously.
- They are created when each node is booted.

- The figure also shows how these path vectors are sent to immediate neighbors after they have been created.

**Fig 4.18 – Path vector**

### Updating Path Vectors

- The **Figure 4.19** below shows the path vector of node C after two events.
- In the first event, node C receives a copy of B's vector, which improves its vector: now it knows how to reach node A.
- In the second event, node C receives a copy of D's vector, which does not change its vector.
- The vector for node C after the first event is stabilized and serves as its forwarding table.

New C	Old C	B	New C	Old C	D
A [C, B, A]	A [ ]	A [B, A]	A [C, B, A]	A [C, B, A]	A [ ]
B [C, B]	B [C, B]	B [B]	B [C, B]	B [C, B]	B [D, B]
C [C]	C [C]	C [B, C]	C [C]	C [C]	C [D, C]
D [C, D]	D [C, D]	D [B, D]	D [C, D]	D [C, D]	D [D]
E [C, E]	E [C, E]	E [ ]	E [C, E]	E [C, E]	E [D, E]

$C[ ] = \text{best}(C[ ], C + B[ ])$

$C[ ] = \text{best}(C[ ], C + D[ ])$

Event 1: C receives a copy of B's vector

Event 2: C receives a copy of D's vector

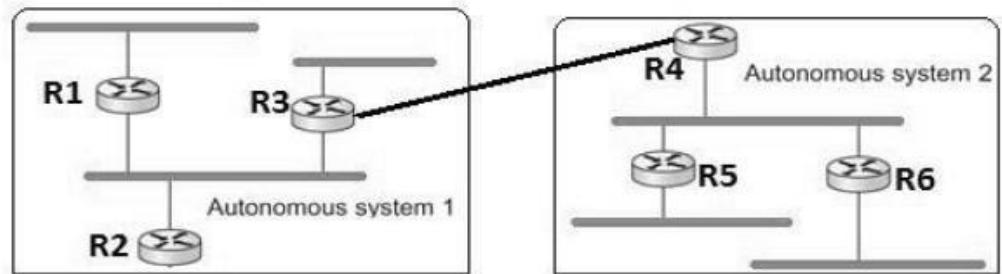
**Fig 4.19 – Path vector of node C**

### BORDER GATEWAY PROTOCOL (BGP)(April/may 2023)(Nov/dec 2023)

- The Border Gateway Protocol version (BGP) is the only interdomain routing protocol used in the Internet today.
- BGP4 is based on the path-vector algorithm. It provides information about

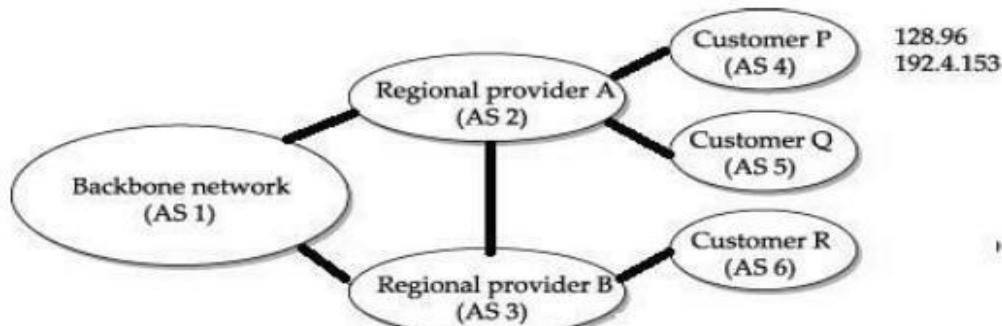
the reachability of networks in the Internet.

- BGP views internet as a set of autonomous systems interconnected arbitrarily. (**Refer Fig 4.20**)



**Fig 4.20 – BGP AS**

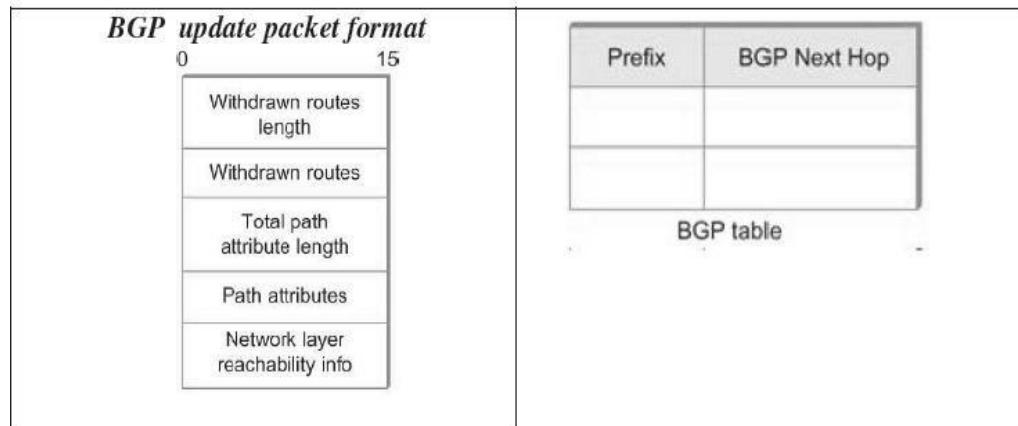
- Each AS have a border router (gateway), by which packets enter and leave that AS. In above figure, R3 and R4 are border routers.
- One of the router in each autonomous system is designated as BGP speaker.
- BGP Speaker exchange reachability information with other BGP speakers, known as external BGP session.
- BGP advertises complete path as enumerated list of AS (path vector) to reach a particular network.
- Paths must be without any loop, i.e., AS list is unique.
- For example, backbone network advertises that networks 128.96 and 192.4.153 can be reached along the path <AS1, AS2, AS4>. (**Refer Fig 4.21**)



**Fig 4.21 – AS**

- If there are multiple routes to a destination, BGP speaker chooses one based on policy.
- Speakers need not advertise any route to a destination, even if one exists.

- Advertised paths can be cancelled, if a link/node on the path goes down. This negative advertisement is known as withdrawn route.
- Routes are not repeatedly sent. If there is no change, keep alive messages are sent. (**Refer Fig 4.22**)



**Fig 4.22 – BGP Packet format**

#### iBGP - interior BGP

- A Variant of BGP. **BGP Packet format**
- Used by routers to update routing information learnt from other speakers to routers inside the autonomous system.
- Each router in the AS is able to determine the appropriate next hop for all prefixes.

#### 6. Discuss the concepts of Multicasting.(April/may 2024)

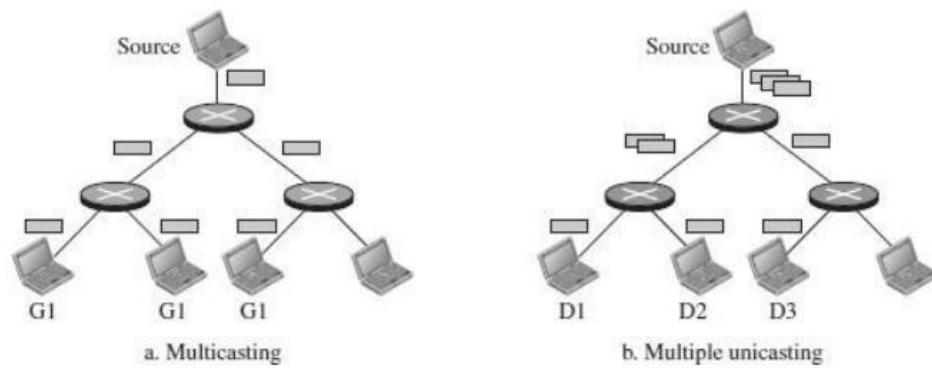
##### Synopsis:

- **INTRODUCTION**
- **IGMP OR MLD PROTOCOL**
- **MULTICAST ADDRESSING**
- **MULTICASTING VERSUS MULTIPLE UNICASTING**
- **NEED FOR MULTICAST**
- **TYPES OF MULTICASTING**
- **MULTICAST APPLICATIONS**

#### INTRODUCTION

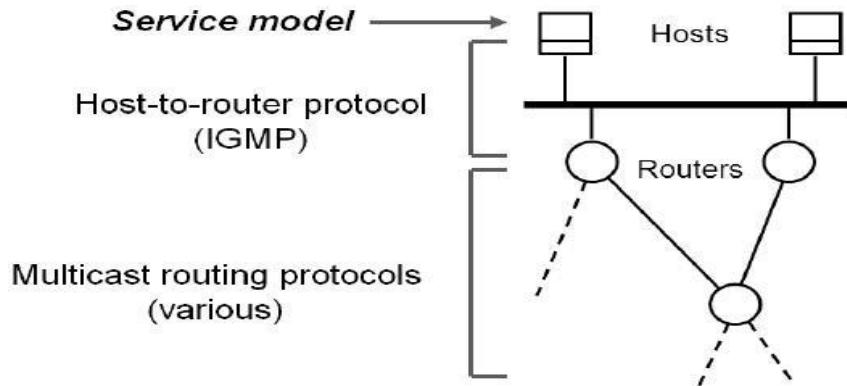
- In multicasting, there is one source and a group of destinations.
  - Multicast supports efficient delivery to multiple destinations.
  - The relationship is one to many or many-to-many.
- ✓ **One-to-Many (Source Specific Multicast)** Radio station broadcast

- Transmitting news, stock-price
  - Software updates to multiple hosts.
- ✓ **Many-to-Many (Any Source Multicast)**
- Multimedia teleconferencing
  - Online multi-player games
  - Distributed simulations.
- In this type of communication, the source address is a unicast address, but the destination address is a group address.
  - The group address defines the members of the group.



**Fig 4.23 – Multicasting**

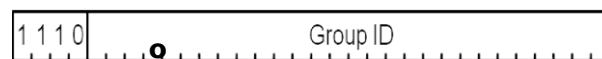
- In multicasting, a multicast router may have to send out copies of the same datagram through more than one interface. (**Refer Fig 4.23**)
  - Hosts that are members of a group receive copies of **Multicasting** any packets sent to that group's multicast address.
  - A host can be in multiple groups.
  - A host can join and leave groups.
  - A host signals its desire to join or leave a multicast group by communicating with its local router using a special protocol. (**Refer Fig 4.24**).
- In IPv4, the protocol is Internet Group Management Protocol (IGMP).
  - In IPv6, the protocol is Multicast Listener Discovery (MLD).

**Fig 4.24 – Service model****IGMP OR MLD PROTOCOL**

- Hosts communicate their desire to join / leave a multicast group to a router using Internet Group Message Protocol (IGMP) in IPv4 or Multicast Listener Discovery (MLD) in IPv6.
- Provides multicast routers with information about the membership status of hosts connected to the network.
- Enables a multicast router to create and update list of loyal members for each group.

**MULTICAST ADDRESSING**

- Multicast address is associated with a group, whose members are dynamic.
- Each group has its own IP multicast address.
- IP addresses reserved for multicasting are Class D in IPv4 (Class D 224.0.0.1 to 239.255.255.255), 1111 1111 prefix in IPv6.



- Hosts that are members of a group receive copy of the packet sent when destination contains group address.

**RANGE OF MULTICAST ADDRESSES**

- An Ethernet multicast physical address is in the range 01 : 00 : 5E : 00 : 00 : 00 to 01 : 00 : 5E : 7F : FF : FF.

**Steps To Convert The Multicast Address To Ethernet Multicast Address.****Step 1 :**

Change the rightmost 3 bytes in hexadecimal.

**Step 2 :**

Subtract 8 from the leftmost digit (obtained in Step 1) , if it is greater than or

equal to 8. If it is less than 8, do not subtract.

**Step 3 :**

Add the result obtained from Step 2 to the Ethernet multicast starting address.

**Example 1:**

Change the multicast IP address 238.212.24.9 to an Ethernet multicast address.

**Solution**

- (1) The rightmost 3 bytes in hexadecimal are D4:18:09.
- (2) We need to subtract 8 from the leftmost digit. The leftmost digit is D, Subtracting 8 from D gives 5. ( $D - 8$ )
- (3) The resulting value will be in 54:18:09.
- (3) We add the result to the Ethernet multicast starting address.

The result is 01:00:5E:54:18:09

**Example 2 :**

Change the multicast IP address 232.43.14.7 to an Ethernet multicast physical address.

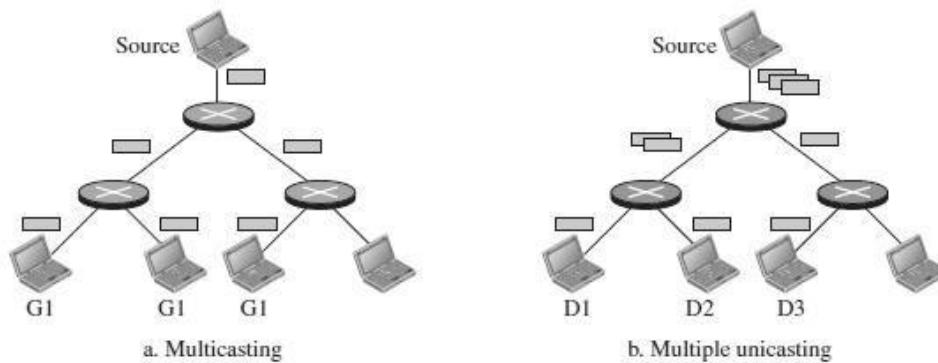
**Solution:**

- (1) The rightmost 3 bytes in hexadecimal are 2B:0E:07.
- (2) We need to subtract 8 from the leftmost digit. The leftmost digit is 2 , which  
is less than 8. So no need to subtract.
- (3) We add the result to the Ethernet multicast starting address.

The result is 01:00:5E:2B:0E:07

**MULTICASTING VERSUS MULTIPLE UNICASTING**

- Multicasting starts with a single packet from the source that is duplicated by the routers. The destination address in each packet is the same for all duplicates.
- Only a single copy of the packet travels between any two routers.

**Fig 4.25 – Multicasting Vs Multiple Unicasting**

- In multiple unicasting, several packets start from the source.
- If there are three destinations, for example, the source sends three packets, each with a different unicast destination address. (**Refer Fig 4.25**)
- There may be multiple copies traveling between two routers.

### NEED FOR MULTICAST

Without support for multicast

- A source needs to send a separate packet with the identical data to each member of the group.
- Source needs to keep track of the IP address of each member in the group.

### Using IP multicast

- Sending host does not send multiple copies of the packet.
- A host sends a single copy of the packet addressed to the group's multicast address.
- The sending host does not need to know the individual unicast IP address of each member.

### TYPES OF MULTICASTING

- Source-Specific Multicast - In source-specific multicast (one-to-many model), receiver specifies multicast group and sender from which it is interested to receive packets. **Example:** Internet radio broadcasts.
- Any Source Multicast - Supplements any source multicast (many-to-many model).

## MULTICAST APPLICATIONS

- Access to Distributed Databases
- Information Dissemination
- Teleconferencing.
- Distance Learning.

**7. Write short notes on multicast routing protocols.**

**Synopsis:**

- MULTICAST ROUTING
- MULTICAST DISTRIBUTION TREES
- MULTICAST ROUTING PROTOCOLS

## MULTICAST ROUTING

- To support multicast, a router must additionally have multicast forwarding tables that indicate, based on multicast address, which links to use to forward the multicast packet.
- Unicast forwarding tables collectively specify a set of paths.
- Multicast forwarding tables collectively specify a set of trees -Multicast distribution trees.
- Multicast routing is the process by which multicast distribution trees are determined.
- To support multicasting, routers additionally build multicast forwarding tables.
- Multicast forwarding table is a tree structure, known as multicast distribution trees.
- Internet multicast is implemented on physical networks that support broadcasting by extending forwarding functions.

## MULTICAST DISTRIBUTION TREES

- There are two types of Multicast Distribution Trees used in multicast routing.
- They are,
  - **Source-Based Tree:** (DVMRP)
  - For each combination of (source , group), there is a shortest path spanning tree.
  - **Flood and prune**

- Send multicast traffic everywhere
- Prune edges that are not actively subscribed to group
- ***Link-state***
  - Routers flood groups they would like to receive
  - Compute shortest-path trees on demand
- **Shared Tree** (PIM)
  - Single distributed tree shared among all sources.
  - Does not include its own topology discovery mechanism, but instead uses routing information supplied by other routing protocols.
  - Specify rendezvous point (RP) for group.
  - Senders send packets to RP, receivers join at RP.
  - RP multicasts to receivers; Fix-up tree for optimization.
  - Rendezvous-Point Tree: one router is the center of the group and therefore the root of the tree.

## MULTICAST ROUTING PROTOCOLS

- Internet multicast is implemented on physical networks that support broadcasting by extending forwarding functions.
- Major multicast routing protocols are:
  1. Distance-Vector Multicast Routing Protocol (DVMRP).
  2. Protocol Independent Multicast (PIM).

### 8. Explain Distance-Vector Multicast Routing Protocol (DVMRP) in multicast routing.(April/may 2014)

**Synopsis:**

- |   |
|---|
| <ul style="list-style-type: none"> <li>➤ <b>Distance Vector Multicast Routing Protocol</b></li> <li>➤ <b>Flooding</b></li> <li>➤ <b>Reverse Path Forwarding (RPF)</b></li> <li>➤ <b>Reverse-Path Broadcasting (RPB)</b></li> <li>➤ <b>Reverse-Path Multicasting (RPM)</b> <ul style="list-style-type: none"> <li>✓ <b>Pruning</b></li> <li>✓ <b>Grafting</b></li> </ul> </li> </ul> |
|---|

### **Distance Vector Multicast Routing Protocol**

- The DVMRP, is a routing protocol used to share information between routers to facilitate the transportation of IP multicast packets among networks.
- It formed the basis of the Internet's historic multicast backbone.
- Distance vector routing for unicast is extended to support multicast routing.
- Each router maintains a routing table for all destination through exchange of distance vectors.
- DVMRP is also known as flood-and-prune protocol.

**DVMRP consists of two major components:**

- A conventional distance-vector routing protocol, like RIP.
- A protocol for determining how to forward multicast packets, based on the routing table.
- DVMRP router forwards a packet if the packet arrived from the link used to reach the source of the packet.
- If downstream links have not pruned the tree.
- DVMRP protocol uses the basic packet types as follows:
  - **DVMRP Probes**
    - for DVMRP Neighbor Discovery
  - **DVMRP Reports**
    - for Multicast Route Exchange
  - **DVMRP Prunes**
    - for pruning multicast delivery trees
  - **DVMRP Grafts**
    - for grafting multicast delivery trees
  - **DVMRP Graft Ack's**
    - for acknowledging graft msgs
- The forwarding table of DVMRP is as follows:

<u>Source Subnet</u>	<u>Multicast Group</u>	<u>TTL</u>	<u>InPort</u>	<u>Out Ports</u>
128.1.0.0	224.1.1.1	200	1 Pr	2p 3p
	224.2.2.2	100	1	2p 3
	224.3.3.3	250	1	2
128.2.0.0	224.1.1.1	150	2	2p 3

- Multicasting is added to distance-vector routing in four stages.

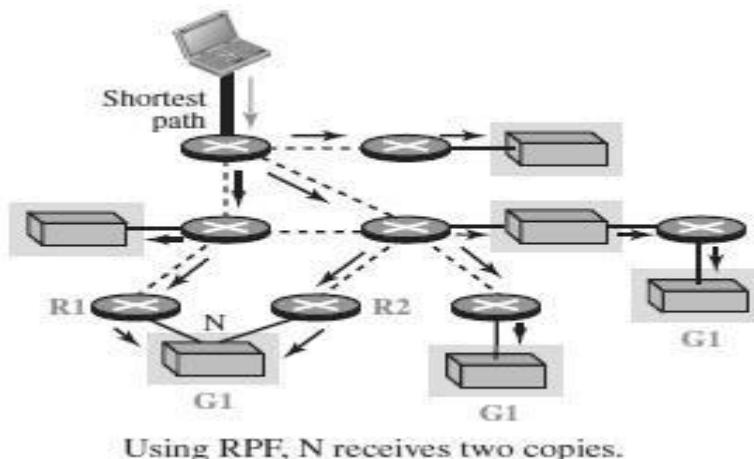
- Flooding.
- Reverse Path Forwarding (RPF).
- Reverse Path Broadcasting (RPB).
- Reverse Path Multicast (RPM).

### Flooding

- Router on receiving a multicast packet from source S to a Destination from Next Hop, forwards the packet on all out-going links.
- Packet is flooded and looped back to S.
- The drawbacks are:
  - ✓ It floods a network, even if it has no members for that group.
  - ✓ Packets are forwarded by each router connected to a LAN, i.e., duplicate flooding.

### Reverse Path Forwarding (RPF)

- RPF eliminates the looping problem in the flooding process.
- Only one copy is forwarded and the other copies are discarded.
- RPF forces the router to forward a multicast packet from one specific interface: the one which has come through the shortest path from the source to the router.
- Packet is flooded but not looped back to S. (**Refer Fig 4.26**)



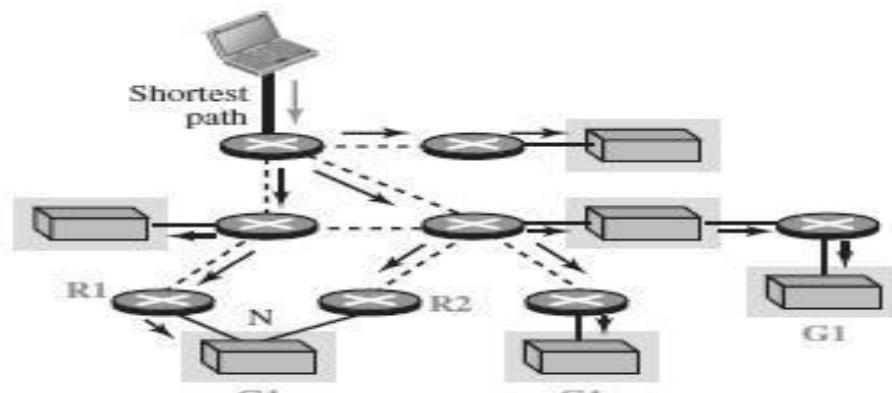
**Fig 4.26 – Reverse Path Forwarding (RPF)**

### Reverse-Path Broadcasting (RPB)

- RPB does not multicast the packet, it broadcasts it.
- RPB creates a shortest path broadcast tree from the source to each destination.
- It guarantees that each destination receives one and only one copy of the packet.
- We need to prevent each network from receiving more than one copy of the packet.
- If a network is connected to more than one router, it may receive a copy of the

packet from each router.

- One router identified as parent called designated Router (DR).
  - Only parent router forwards multicast packets from source S to the attached network.
  - When a router that is not the parent of the attached network receives a multicast packet, it simply drops the packet. **(Refer Fig 4.27)**



Using RPB, N receives only one copy.

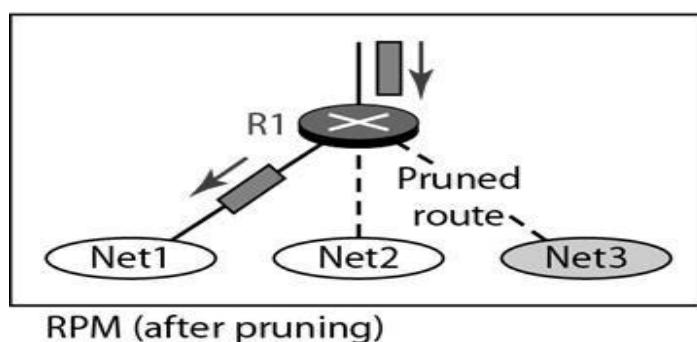
**Fig 4.27 – Reverse-Path Broadcasting (RPB)**

#### Reverse-Path Multicasting (RPM)

- To increase efficiency, the multicast packet must reach only those networks that have active members for that particular group.
- RPM adds pruning and grafting to RPB to create a multicast shortest path tree that supports dynamic membership changes.

#### Pruning:

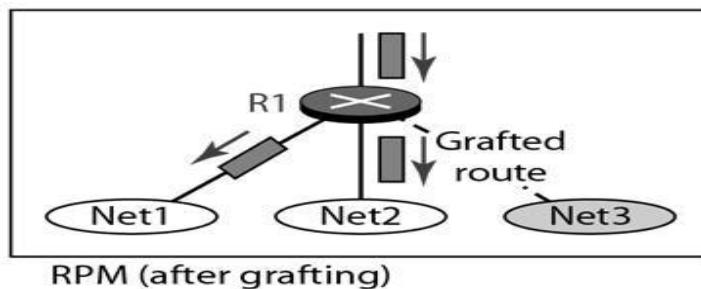
- Sent from routers receiving multicast traffic for which they have no active group members “Prunes” the tree created by DVMRP.
- Stops needless data from being sent **(Refer Fig 4.28)**



**Fig 4.28 – Reverse-Path Multicasting (RPM) - Pruning**

**Grafting:**

- Used after a branch has been pruned back (**Refer Fig 4.29**)
- Sent by a router that has a host that joins a multicast group.
- Goes from router to router until a router active on the multicast group is reached.
- Sent for the following cases.
  - A new host member joins a group.
  - A new dependent router joins a pruned branch.
  - A dependent router restarts on a pruned branch

**Fig 4.29 – Reverse-Path Multicasting (RPM) - Grafting****9. Explain Protocol Independent Multicast (PIM) in multicast routing.****Synopsis:**

- **Protocol Independent Multicast (PIM)**
- **Shared Tree**
- **Source-Specific Tree**
- **Analysis of PIM**

**Protocol Independent Multicast (PIM)**

- PIM divides multicast routing problem into sparse and dense mode.
- PIM sparse mode (PIM-SM) is widely used.
- PIM does not rely on any type of unicast routing protocol, hence protocol independent.
- Routers explicitly join and leave multicast group using Join and Prune messages.
- One of the router is designated as rendezvous point (RP) for each group in a domain to receive PIM messages.
- Multicast forwarding tree is built as a result of routers sending Join messages to RP.

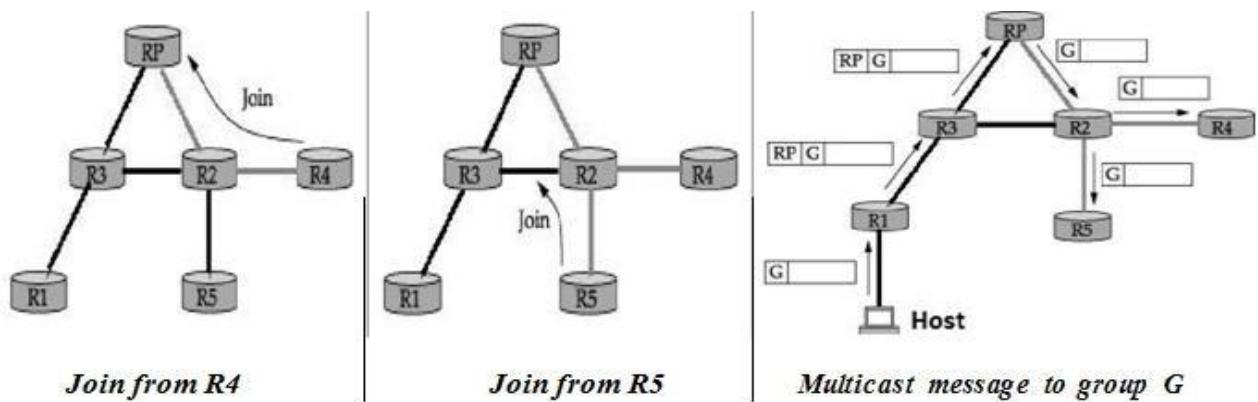
- Two types of trees to be constructed:
  - **Shared tree** - used by all senders.
  - **Source-specific tree** - used only by a specific sending host.
- The normal mode of operation creates the shared tree first, followed by one or more source-specific trees.

### **Shared Tree**

- When a router sends Join message for group G to RP, it goes through a set of routers.
- Join message is wildcarded (\*), i.e., it is applicable to all senders.
- Routers create an entry (\*, G) in its forwarding table for the shared tree.
- Interface on which the Join arrived is marked to forward packets for that group.
- Forwards Join towards rendezvous router RP.
- Eventually, the message arrives at RP. Thus a shared tree with RP as root is formed.

### **Example**

- Router R4 sends Join message for group G to rendezvous router RP. (**Refer Fig 4.30**)
- Join message is received by router R2. It makes an entry (\*, G) in its table and forwards the message to RP.



- When R5 sends Join message for group G, R2 does not forwards the Join. It adds an outgoing interface to the forwarding table created for that group.

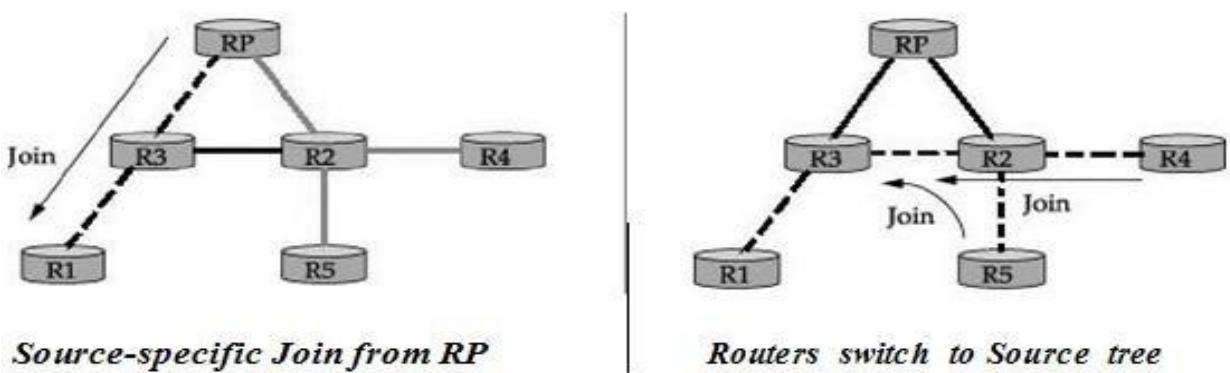
**Fig 4.30 – PIM – Shared Tree**

- As routers send Join message for a group, branches are added to the tree, i.e., shared.
- Multicast packets sent from hosts are forwarded to designated router RP.
  - Suppose router R1, receives a message to group G. If R1 has no state for group G.
    - Encapsulates the multicast packet in a Register message.
    - Multicast packet is tunneled along the way to RP.
- RP decapsulates the packet and sends multicast packet onto the shared tree, towards R2.
- R2 forwards the multicast packet to routers R4 and R5 that have members for group G.

### Source-Specific Tree

- RP can force routers to know about group G, by sending Join message to the sending host, so that tunneling can be avoided.
- Intermediary routers create sender-specific entry (S, G) in their tables. Thus a source-specific route from R1 to RP is formed.
- If there is high rate of packets sent from a sender to a group G, then shared- tree is replaced by source-specific tree with sender as root. (**Refer Fig 4.31**)

*Example*



**Fig 4.31 – PIM – Source specified tree**

- Rendezvous router RP sends a Join message to the host router R1.
- Router R3 learns about group G through the message sent by RP.
- Router R4 send a source-specific Join due to high rate of packets from sender.
- Router R2 learns about group G through the message sent by R4.
- Eventually a source-specific tree is formed with R1 as root.

**Analysis of PIM**

- Protocol independent because, tree is based on Join messages via shortest path.
- Shared trees are more scalable than source-specific trees.
- Source-specific trees enable efficient routing than shared trees.

**10. Write about Flow control and Buffering?(April/may2023)****Flow Control**

- Flow control is a mechanism used in computer networks to match the sender's data transmission rate with the receiver's capacity to process that data. In the absence of effective flow control, the receiver may become overloaded, resulting in data loss or retransmissions that can degrade overall network performance.
- For example, if a sender is capable of transmitting data at 100 Mbps but the receiver can only handle 50 Mbps, the excess data will fill up the receiver's buffer and eventually overflow, leading to packet loss. Flow control ensures that such mismatches are managed gracefully.

**Significance of Flow Control**

Flow control is critical for maintaining reliable communication in networks for several reasons:

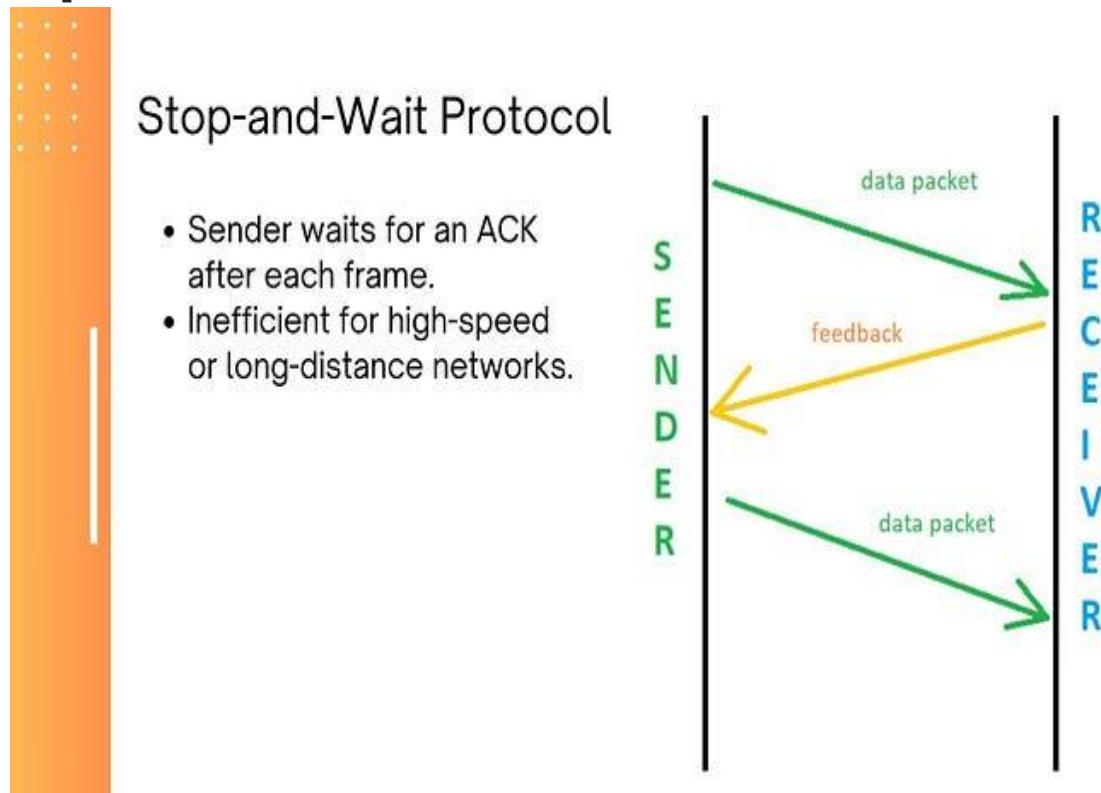
1. **Prevents Buffer Overflow:** By regulating the sender's rate, it ensures that the receiver's buffer does not overflow, avoiding packet loss.
2. **Optimizes Resource Utilization:** Ensures efficient use of network resources by maintaining a steady flow of data.
3. **Improves Reliability:** Reduces the need for retransmissions caused by dropped packets, enhancing the reliability of the communication.

4. **Supports Diverse Devices:** Handles communication between devices with varying processing speeds and buffer capacities.

### Techniques for Flow Control

Several techniques are employed in flow control to achieve efficient and reliable communication. The most commonly used methods are discussed below.

#### Stop-and-Wait Protocol



**Figure 4.32 Stop-and-Wait Protocol**

The Stop-and-Wait Protocol is the simplest form of flow control as shown in figure 4.32. In this method:

- The sender transmits one data frame/packet and then pauses to wait for an acknowledgment (ACK) from the receiver.
- Upon receiving the acknowledgment, the sender sends the next frame.

This approach ensures that the receiver processes each frame before the sender sends more data. While simple, it is inefficient in high-speed or long-distance networks because the sender remains idle during the acknowledgment delay.

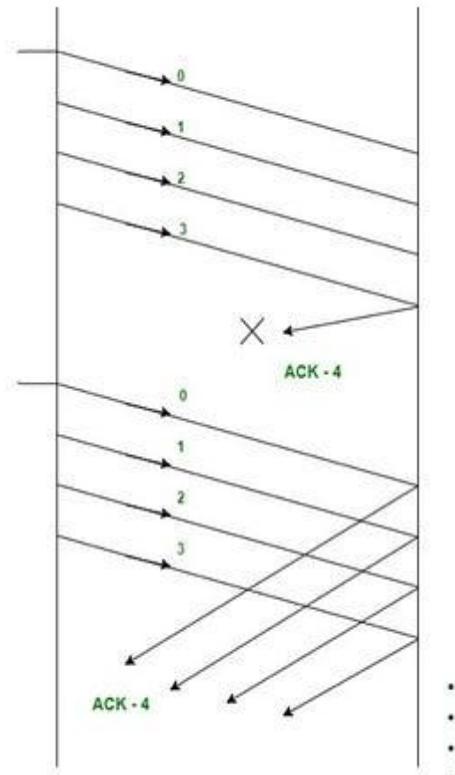
**Example:** If a sender transmits Frame/packet 1, it waits for the acknowledgment of Frame 1 before proceeding to Frame 2. Any delay in acknowledgment, whether due to network latency or other factors, reduces throughput.

### Sliding Window Protocol



### Sliding Window Protocol

- How It Works: Sender sends multiple frames before waiting for ACKs.
- Benefit: Increases throughput by minimizing idle time.



**Figure 4.33 Sliding Window Protocol**

The Sliding Window Protocol improves efficiency by allowing the sender to transmit multiple frames/packets before waiting for acknowledgments. It is based on the concept of a “window” that defines the range of frames the sender can send without waiting for an acknowledgement.

- The sender maintains a **sender window**, which keeps track of the frames sent but not yet acknowledged.
- The receiver maintains a **receiver window**, which tracks the frames it can accept and process.
- As acknowledgments are received, the window “slides” forward, allowing the sender to transmit more frames.

This method minimizes idle time and maximizes throughput.

**Example:** If the window size is set to 4, the sender can transmit Frames 1, 2, 3, and 4 without waiting. Upon acknowledgment of Frame/packet 1, the window slides forward, allowing the sender to transmit Frame 5.

### Credit-Based Flow Control

In credit-based flow control, the receiver issues “credits” or tokens that represent its readiness to process a specific number of frames.

- The sender can only transmit data equivalent to the number of credits it has.
- Each credit ensures the receiver’s buffer has enough space to handle the corresponding frame.

This mechanism ensures that the sender does not overload the receiver’s buffer and is often used in high-reliability environments such as Fibre Channel networks.

### Rate-Based Flow Control

Rate-based flow control involves regulating the sender’s data transmission rate based on the receiver’s capacity.

- The receiver communicates its maximum acceptable data rate to the sender.
- The sender adjusts its transmission speed accordingly.

This approach is particularly useful in real-time applications where maintaining a specific transmission rate is essential for ensuring data quality, such as streaming media.

### Challenges in Flow Control

Flow control mechanisms must address several challenges to function effectively:

1. **Network Latency:** High latency can delay acknowledgments, affecting the performance of protocols like Stop-and-Wait.
2. **Varying Network Speeds:** Differences in sender and receiver speeds require adaptive mechanisms.
3. **Dynamic Network Conditions:** Changing network conditions, such as congestion, can impact flow control effectiveness.

4. **Scalability:** In large-scale networks, managing flow control across multiple devices and connections becomes complex.

### **Buffering**

In Buffering, the communication is direct or indirect, message exchanged by communicating processes reside in a temporary queue. Buffering is typically used to manage data flow between devices and helps regulate the rate of data transfer. The buffer allows the sender to transmit data at a faster rate while the receiver processes the data at its own pace.

#### **Types of Buffering:**

1. **Zero Capacity** – This queue cannot keep any message waiting in it. Thus it has maximum length 0. For this, a sending process must be blocked until the receiving process receives the message. It is also known as no buffering.
2. **Bounded Capacity** – This queue has finite length n. Thus it can have n messages waiting in it. If the queue is not full, new message can be placed in the queue, and a sending process is not blocked. It is also known as automatic buffering.
3. **Unbounded Capacity** – This queue has infinite length. Thus any number of messages can wait in it. In such a system, a sending process is never blocked.

#### **Need of Buffering :**

- It helps in matching speed between two devices, between which the data is transmitted. For example, a hard disk has to store the file received from the modem.
- It helps the devices with different data transfer size to get adapted to each other.
- It helps devices to manipulate data before sending or receiving.
- It also supports copy semantics.

#### **How buffering works:**

When a device receives a data packet, it first checks to see if there is enough space in its input buffer to store the packet. If there is not enough space, the packet may be dropped or lost, leading to performance issues.

Assuming there is enough space in the input buffer, the packet is stored temporarily until it can be processed or forwarded to its destination. The device may also apply certain policies or rules to the packet, such as quality of service (QoS) rules, before forwarding it.

Output buffering works in a similar way, with packets being stored temporarily in a buffer until they can be transmitted to their destination. In this case, the buffer ensures that packets are transmitted in the correct order and without delay.

#### **Buffering provides several advantages:**

- Regulating data flow between devices
- Allowing the sender to transmit data at a faster rate
- Preventing lost data due to network congestion

**Disadvantages buffering:**

- Increased latency due to the time it takes to store and retrieve data from the buffer
- Increased memory usage due to the buffer's storage requirements



(Approved by AICTE, New Delhi, Affiliated to Anna University Chennai, Accredited by NBA, TCS & NAAC - 'A' Grade)

## DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND DATA SCIENCE

II YEAR / IV SEM

### CS3591 – COMPUTER NETWORKS

#### UNIT V – DATA LINK AND PHYSICAL LAYERS

Data Link Layer – Framing – Flow control – Error control – Data-Link Layer Protocols – HDLC – PPP - Media Access Control – Ethernet Basics – CSMA/CD – Virtual LAN – Wireless LAN (802.11) - Physical Layer: Data and Signals - Performance – Transmission media- Switching – Circuit Switching

#### PART-A

##### **1. What are the responsibilities of data link layer?**

Specific responsibilities of data link layer include the following.

- a) Framing.
- b) Physical addressing.
- c) Flow control.
- d) Error control.
- e) Access control.

##### **2. Define flow control. (NOV 2011)(May 2015) (May 2016)**

Flow control refers to a set of procedures used to **restrict the amount of data**. The sender can send before waiting for acknowledgment.

##### **3. Mention the categories of flow control.**

There are 2 methods have been developed to control flow of data across communication links.

- a) Stop and wait - send one frame at a time.
- b) Sliding window - send several frames at a time.

**4. What do you meant by error control? (NOV 2010)(May 2015)**

Error control is used for **detecting and retransmitting damaged or lost frames** and to prevent duplication of frames. This is achieved through a trailer added at the end of the frame.

**5. Define Error detection. (NOV 2011)**

**Data can be corrupted during transmission. For reliable communication, errors must be detected and corrected**

Types of error:

- ✓ Single bit error.
- ✓ Burst error.

The three error detecting techniques are:

- Parity check.
- Check sum algorithm.
- Cyclic Redundancy Check.

**6. What is the use of two dimensional parity in error detection? (NOV 2012)**

- It is based on simple parity.
- It performs calculation for each bit position across each byte in the frame.
- This adds extra parity byte for entire frame, in addition to a parity bit for each byte.

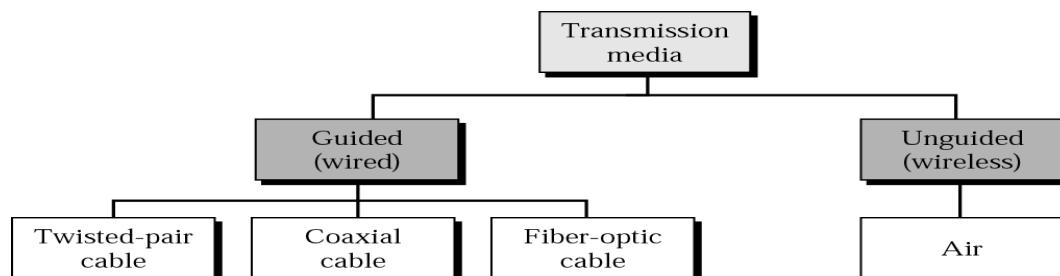
**7. What are the issues (Services) in data link layer?**

- a) Framing
- b) Error Control
- c) Flow Control

**8. List the types of transmission media.(Nov 2021)**

Communication can be made by 2 ways

1. Guided (Wired)
  - i. Unguided (Wireless)



**9.What do you mean by framing? (Nov/Dec 2013) (Nov/Dec 2014)**

**Frames are the small data units** created by data link layer and the process of creating frames by the data link layer is known as framing.

**10.Define (or) mechanism of stop and wait protocol. (Nov 2016)**

The idea of stop-and-wait is straightforward: **After transmitting one frame, the sender waits for an acknowledgment before transmitting the next frame.** If the acknowledgment does not arrive after a certain period of time, the sender times out and retransmits the original frame.

**11. Define sliding window algorithm.**

**The sender can transmit several frames before needing an acknowledgement.** Frames can be sent one right after another meaning that the link can carry several frames at once and its capacity can be used efficiently. The receiver acknowledges only some of the frames, using a single ACK to confirm the receipt of multiple data frames.

**12. Define switching & list its types.****Switching**

- To make communication among multiple devices efficiently, a process used is called switching.
- A switched **network** consists of a **series of interlinked nodes** called switches.

**Type of switching**

- Circuit Switching
- Packet Switching
- Message Switching

**13. Write down any two differences between circuit switching and packet switching. (Nov/Dec 2020) (May 2017)****Circuit switching**

- In circuit switching network dedicated channel has to be established before the call is made between users.
- The channel is reserved between the users till the connection is active.

**Packet switching**

- In packet switching network unlike CS network, it is not required to establish the connection initially.
- The connection/channel is available to use by many users.

**14. Define bit stuffing. Give example (MAY 2011) (May 2017)**

Bit stuffing is the **insertion of one or more bits** into a transmission unit as a way to provide signaling information to a receiver. The receiver knows how to detect and remove or disregard the stuffed bits.

- e.g, Sending side - 011111010

**15.What is Ethernet?**

Ethernet is a multiple-access network, meaning that a set of nodes send and receive frames over a shared link.

**16.What are the four prominent wireless technologies?**

- Bluetooth
- Wi-Fi(formally known as 802.11)
- WiMAX(802.16)
- Third generation or 3G cellular wireless.

**17.Define Bluetooth. (May 2016)**

Bluetooth is a network technology that connects mobile devices wirelessly over a short-range to form a personal area network (PAN). They use short-wavelength, ultra-high frequency (UHF) radio waves within the range 2.400 to 2.485 GHz, for wireless communications.

**Bluetooth Usage:**

- Access Points for Data and Voice – Real-time voice and data transmissions are provided by Bluetooth by connecting portable and stationary network devices wirelessly.

**18. What is the use of Switch?**

It is used to forward the packets between shared media LANs such as Ethernet. Such switches are sometimes known by the obvious name of LAN switches.

**19. What is meant by circuit switching? (NOV/DEC 2010) ,(April/may/2023)**

Circuit switching is a process that establishes connections on demand and permits exclusive use of those connections until released. Connect mobile phones to a headset, or a notebook computer to a printer.

**20. What is High Level data link control? (Nov 2021)**

High-level Data Link Control (HDLC) is a group of communication protocols of the data link layer for transmitting data between network points or nodes. Since it is a data link protocol, data is organized into frames. A frame is transmitted via the network to the destination that verifies its successful arrival. It is a bit - oriented protocol that is applicable for both point - to - point and multipoint communications

**21. Differentiate fast Ethernet and gigabit Ethernet. (NOV/DEC 2012)**

- Fast Ethernet cards connect to networks at a rate of 100 Mbps while Gigabit network cards can connect at speeds up to 1000mb/s.
- The main difference between the two is speed.
- A fast Ethernet card can run on bandwidths at 100mb/s while a gigabit Ethernet can run at ten times that speed.
- However, the existence of FDDIs around made this technology more like a stepping stone to something better – enter the gigabit card.
- Gigabit networks are made to run the best at Layer 3 switching meaning it has more route functionality than the 100mbps fast Ethernet.

**22. What do you understand by CSMA protocol? (May 2015)**

Carrier Sense Multiple Access is a probabilistic Media Access control (MAC) protocol in which a node verifies the absence of other traffic before transmitting on a shared transmission medium, such as an electrical bus.

**23. Differentiate persistent and non persistent CSMA. (Nov/Dec 2014)**

- In 1-persistent CSMA if the medium is busy, the channel will be sensed until it is idle, then it will transmit immediately. This means that collisions are almost guaranteed to occur.
- In non-persistent CSMA if the medium is busy, there will be a random delay for retransmission.
- This reduces the probability of collisions, but wastes the capacity.

**24. What are the functions of MAC?**

MAC sub layer resolves the contention for the shared media. It contains synchronization, flag, flow and error control specifications necessary to move information from one place to another, as well as the physical address of the next station to receive and route a packet.

**25. List the Types of Error and explain briefly.**

- Single-Bit Error
- Burst Error

**Single-Bit Error**

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

( In a single-bit error, only 1 bit in the data unit has changed.)

**Burst Error**

The term *burst error* means that 2 or more bits in the data unit have changed from 1 to 0 or from 0 to 1.

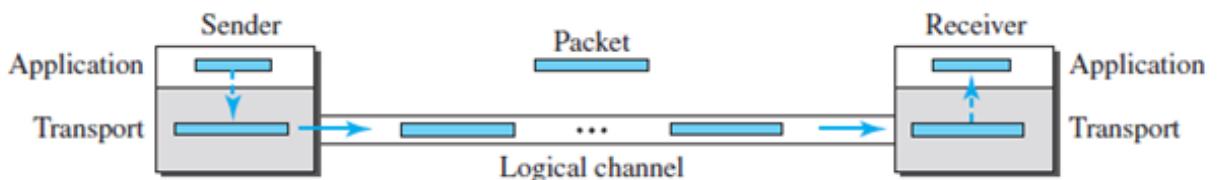
(A burst error means that 2 or more bits in the data unit have changed.)

**PART-B****1. Discuss the protocols used in data link layer.****Synopsis:**

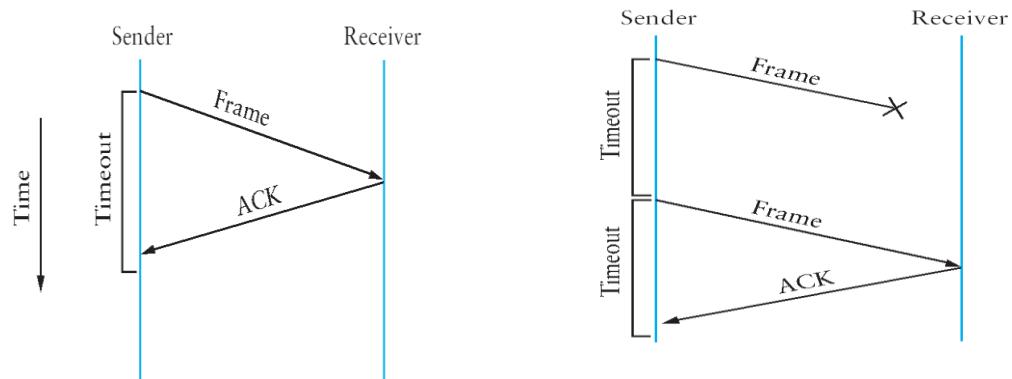
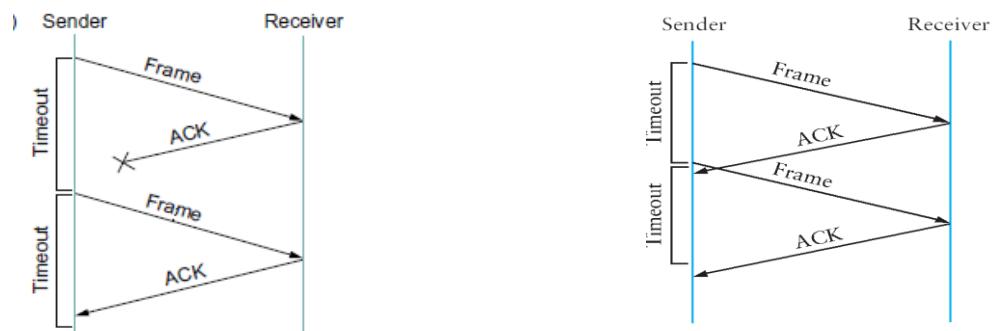
- **Simple Protocol**
- **Stop-and-Wait Protocol**
- **Piggybacking**

**Simple Protocol**

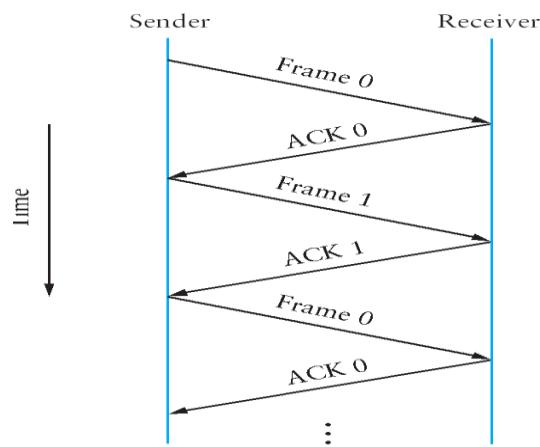
- Our first protocol is a simple connectionless protocol with neither flow nor error control.
- We assume that the receiver can immediately handle any packet it receives. In other words, the receiver can never be overwhelmed with incoming packets. (Refer fig 5.1)

**Fig 5.1 – Simple protocol****Stop and Wait Protocol**

- After transmitting one frame, the sender waits for an acknowledgment before transmitting the next frame.
- If the acknowledgment does not arrive after a certain period of time, the sender times out and retransmit the original frame. (Refer fig 5.2).

**a) The ACK is received before the timer expires****b) The original frame is lost****c) The ACK is lost****d) The timeout fires too soon****fig 5.2- Stop and Wait Protocol**

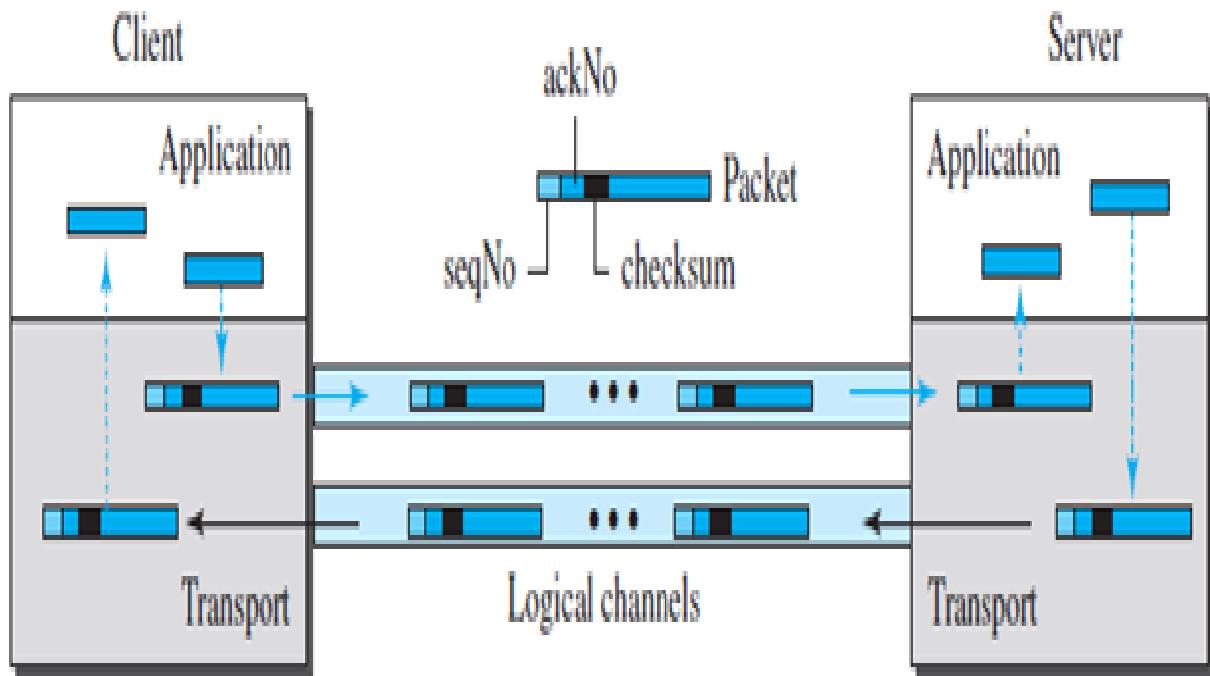
- Fig: illustrates four different scenarios that result from this basic algorithm.
  - The sending side is represented on the left, the receiving side is depicted on the right, and time flows from top to bottom.
- In Fig (a) ACK is received before the timer expires, (b) and (c) show the situation in which the original frame and the ACK, respectively, are lost, and (d) shows the situation in which the timeout fires too soon..

**Fig 5.3 – Normal operation**

- Suppose the sender sends a frame and the receiver acknowledges it, but the acknowledgment is either lost or delayed in arriving. This situation is in (c) and (d). In both cases, the sender times out and retransmit the original frame, but the receiver will think that it is the next frame, since it correctly received and acknowledged the first frame.
- This makes the receiver to receive the duplicate copies. To avoid this two sequence numbers (0 and 1) must be used alternatively. (Refer fig 5.3)
- The main drawback of the stop-and-wait algorithm is that it allows the sender have Only one outstanding frame on the link at a time.

#### **Bidirectional Protocols: Piggybacking**

- The four protocols we discussed earlier in this section are all unidirectional: data packets flow in only one direction and acknowledgments travel in the other direction.
- In real life, data packets are normally flowing in both directions: from client to server and from server to client.
- This means that acknowledgments also need to flow in both directions.
- A technique called **piggybacking** is used to improve the efficiency of the bidirectional protocols. When a packet is carrying data from A to B, it can also carry acknowledgment feedback about arrived packets from B; when a packet is carrying data from B to A, it can also carry acknowledgment feedback about the arrived packets from A. (Refer fig 5.4)



**Fig 5.4 – Design of piggybacking in Go-Back-N**

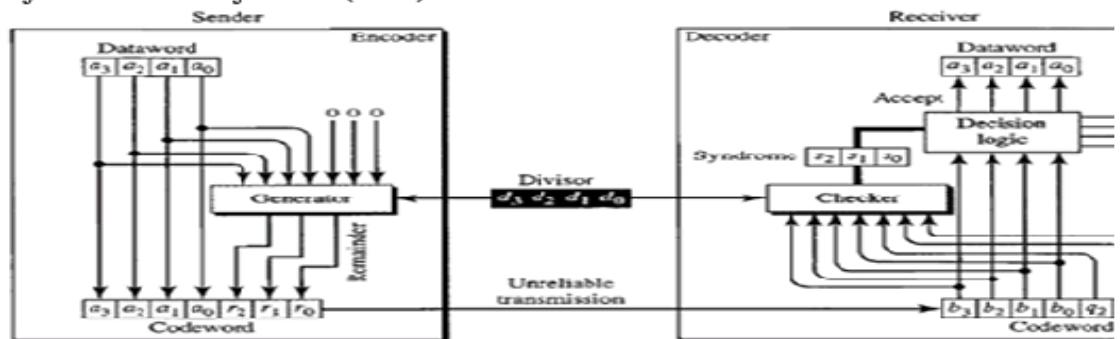
**2. Illustrate the working of CRC code with  $C(7, 4)$  , Where  $n = 7$ ,  $k = 4$ , Codeword = 1001110. Give the division in the CRC decoder for two cases.**

- (i) Dataword accepted (ii) Dataword Discarded

**Synopsis:**

- **CRC Encoder**
- **Decoder**

### Cyclic Redundancy Check (CRC)



CRC is used in networks such as LANs and WANs. We can create cyclic codes to correct errors. The above figure is a possible design for the encoder and decoder.

#### CRC Encoder

- In the encoder, the dataword has **k bits** and the codeword has **n bits**.
- The size of the dataword is augmented by adding **(n - k) number of 0's** to the right-hand side of the word.
- The **n-bit** result is fed into the generator.
- The generator uses a divisor of size **n - k + 1** predefined and agreed by both sender and receiver.
- The quotient of the division is discarded;
- The remainder ( $r_2 r_1 r_0$ ) is appended to the dataword to create the codeword.

Let us take

**k=4 bits**

**n=7 bits**

Appended Dataword Size = **(n-k) = 3**.

Divisor Size = **(n-k+1) = 4**.

#### Decoder

- The decoder receives the possibly corrupted codeword.
- A copy of all **n bits** is fed to the checker which is a replica of the generator.
- The remainder produced by the checker is a syndrome of **n - k** (3 here) bits, which is fed to the decision logic analyzer. The analyzer has a simple function.
- If the syndrome bits are all 0's, the 4 leftmost bits of the codeword are accepted as the dataword (interpreted as no error); otherwise, the 4 bits are discarded (error).

**Example: A CRC code with C(7, 4)**

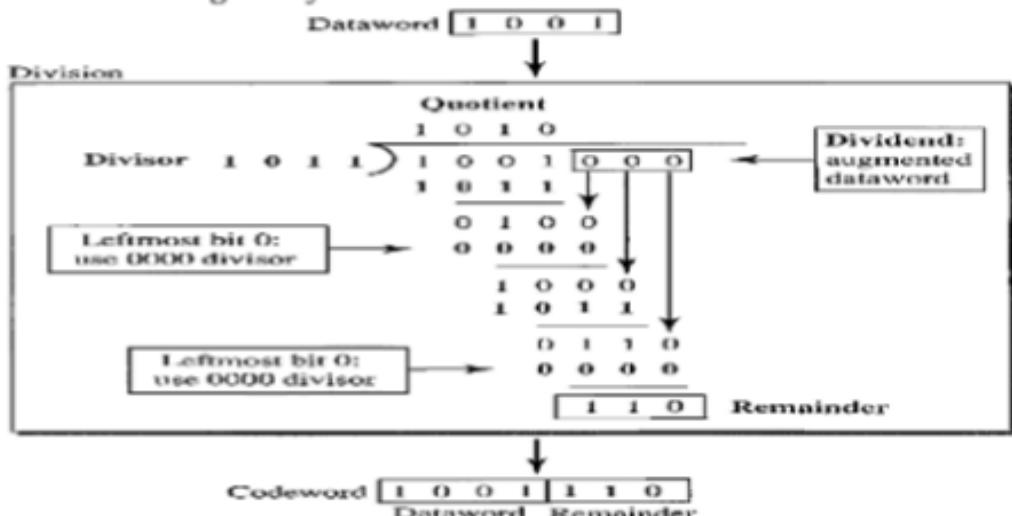
Dataword	Codeword	Dataword	Codeword
0000	0000000	1000	1000101
0001	0001011	1001	1001110
0010	0010110	1010	1010011
0011	0011101	1011	1011000
0100	0100111	1100	1100010
0101	0101100	1101	1101001
0110	0110001	1110	1110100
0111	0111010	1111	1111111

In the above table the dataword size is 4 and codeword size is 7. Codeword can be obtained by applying the CRC procedure as we mentioned above. Now let us check for the dataword 1001, and how we get codeword 1001110.

**Encoder**

The encoder takes the dataword and augments it with  $(n - k)$  number of 0's. It then divides the augmented dataword by the divisor. Let us take the divisor 1011.

The value 1011 will agree by both sender and receiver.



Note: We use XOR operation in the above division.

- As in decimal division, the process is done step by step.
- In each step, a copy of the divisor is XORed with the 4 bits of the dividend.
- The result of the XOR operation (remainder) is 3 bits is used for the next step after 1 extra bit is pulled down to make it 4 bits long.
- If the leftmost bit of the dividend is 0, the step cannot use the regular divisor; we need to use an all-0's divisor.
- When there are no bits left to pull down, we have a result.
- The 3-bit remainder forms the check bits ( $r_2 r_1 r_0$ ). They are appended to the dataword to create the codeword.

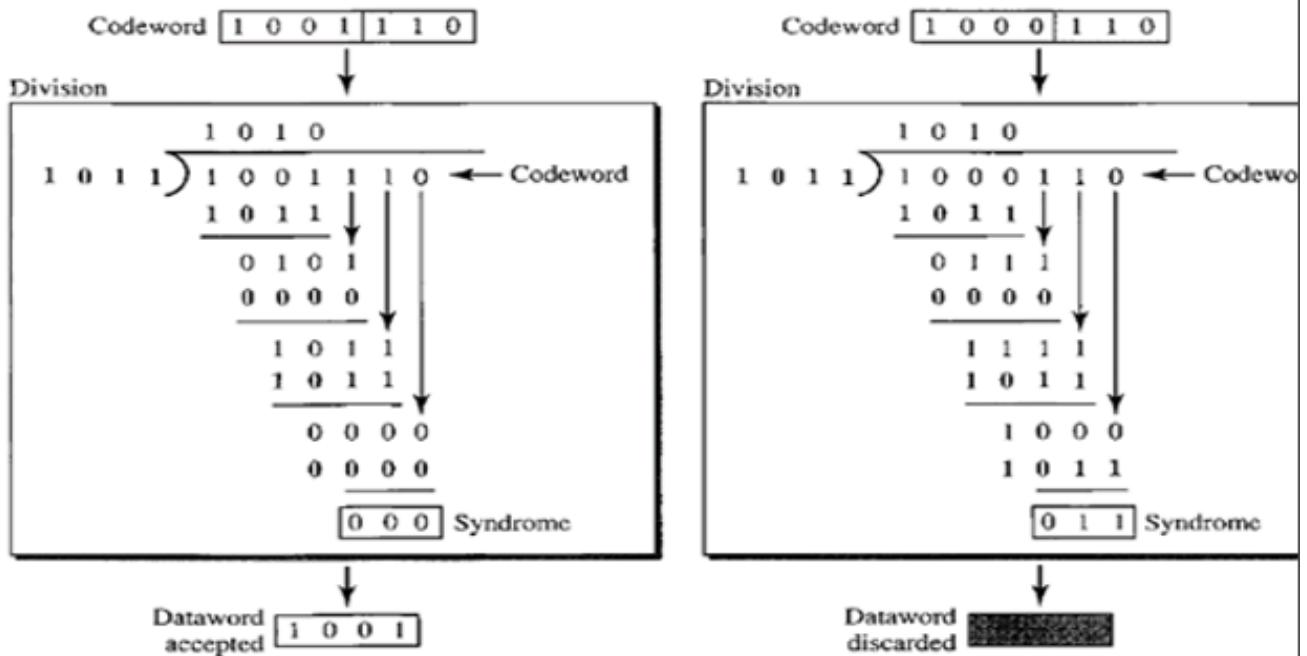
**Decoder**

- The codeword can change during transmission.
- The decoder does the same division process as the encoder.

- The remainder of the division is the syndrome.
- If the syndrome is all 0's, there is no error; the dataword is separated from the received codeword and accepted. Otherwise, everything is discarded.

The below figure shows two cases:

- The left-hand figure shows the value of syndrome when no error has occurred; the syndrome is 000.
- The right-hand part of the figure shows the case in which there is one single error. The syndrome is not all 0's (it is 011).



### 3. Discuss physical links (or) transmission media (or) how communication made by network? ,Types of transmission media?(April/may 2024)

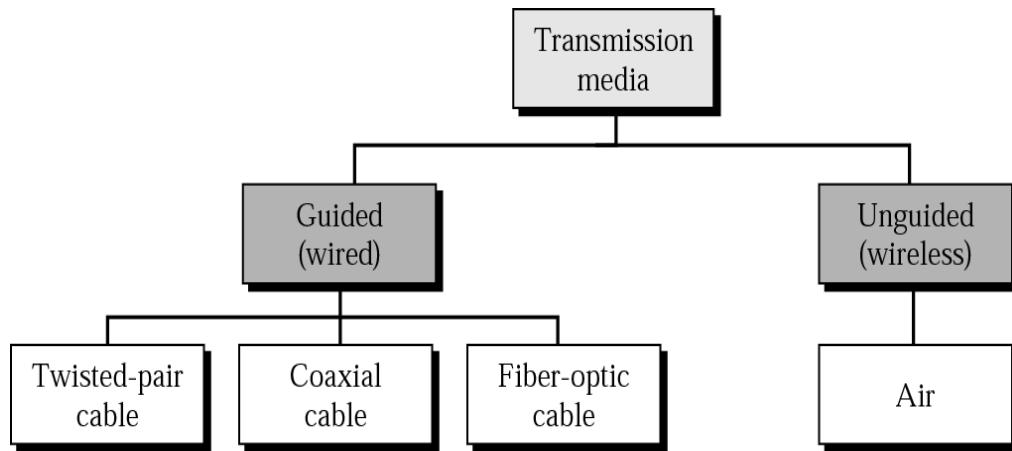
#### Synopsis:

- Communication can be made by 2 ways (Refer fig 5.5)
- Guided (Wired)

1. Twisted Pair Cable
2. Coaxial Cable
3. Fiber Optic Cable

- Unguided (Wireless)

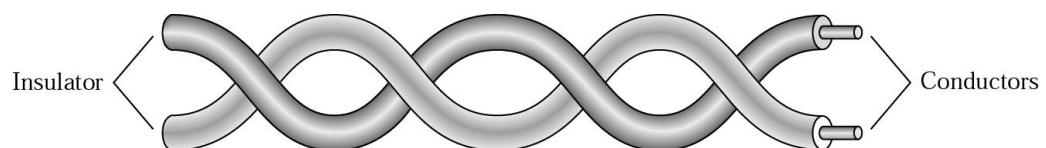
1. Radio Waves
2. Microwaves
3. Infrared

**Fig 5.5 – Transmission media types****Guided Media**

- Guided media conduct signals from one device to another include Twisted-pair cable, Coaxial Cable and Fiber-optic cable.
- A signal traveling along any of these media is directed and contained by the physical limits of the medium.
- Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current.
- Optical fiber is a glass cable that accepts and transports signals in the form of light.

**Twisted Pair Cable**

- A twisted pair consists of two conductors (normally copper) each with its own plastic insulation, twisted together. (Refer fig 5.6)
  - One of the wires is used to carry signals to the receiver
  - Other is used as ground reference

**Fig 5.6 – Twisted pair cable**

- Interference and cross talk may affect both the wires and create unwanted signals, if the two wires are parallel.
- By twisting the pair, a balance is maintained. Suppose in one twist one wire is closer to noise and the other is farther in the next twist the reverse is true.

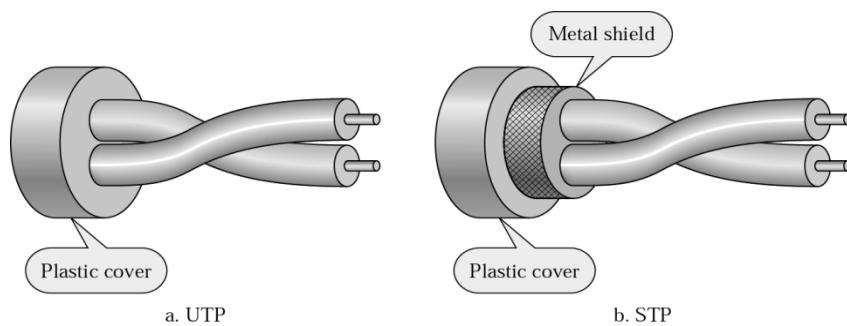
- Twisting makes it probable that both wires are equally affected by external influences.

**Twisted Pair Cable comes into two forms:** (Refer fig 5.7)

- **Unshielded**
- **Shielded**

#### **Unshielded versus shielded Twisted-Pair Cable**

- Shielded Twisted-Pair (STP) Cable has a metal foil or braided-mesh covering that encases each pair of insulated conductors.
- Metal casing improves that quality of cable by preventing the penetration of noise or cross talk.
- It is more expensive. The following figure shows the difference between UTP and STP.



**Fig 5.7 – Unshielded Vs Shielded**

#### **Applications**

- Twisted Pair cables are used in telephone lines to provide voice and data channels.
- Local area networks also use twisted pair cables.

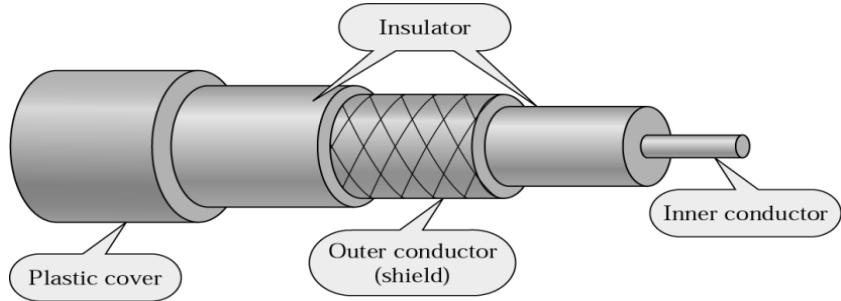
#### **Connectors**

- The most common UTP connector is RJ45.

#### **Coaxial Cable**

- Coaxial cable (coax) carries signals of higher frequency ranges than twisted pair cable.
- Instead of having two wires, coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, and with outer conductor of metal foil.

- The outer metallic wrapping serves both as a shield against noise and as the second conductor and the whole cable is protected by a plastic cover. (Refer fig 5.8)



**Fig 5.8 – Coaxial cable**

#### Categories of coaxial cables

Category	Impedance	Use
RG-59	75	Cable TV
RG-58	50	Thin Ethernet
RG-11	50	Thick Ethernet

**Table 5.1 - Coaxial cables**

#### Applications

- It is used in analog and digital telephone networks
- It is also used in Cable TV networks
- It is used in Ethernet LAN

#### Connectors

- BNC connector – to connect the end of the cable to a device
- BNC T - to branch out network connection to computer
- BNC terminator - at the end of the cable to prevent the reflection of the signal.

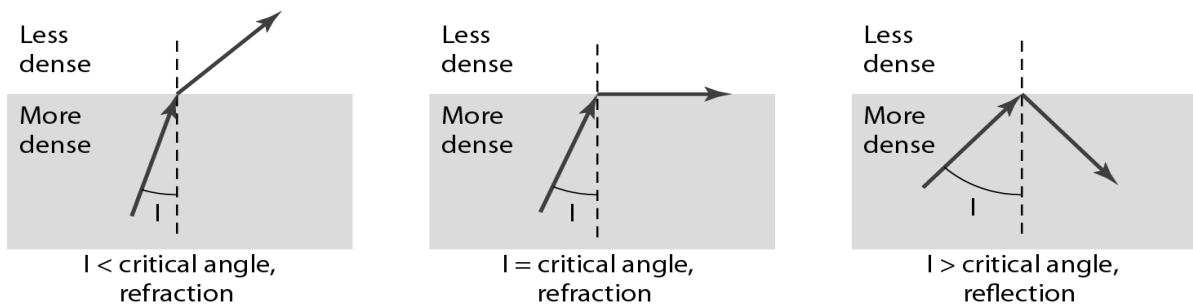
#### Fiber Optic Cable

- A fiber-optic cable is made of glass or plastic and transmits signals in the form of light.

#### Properties of light

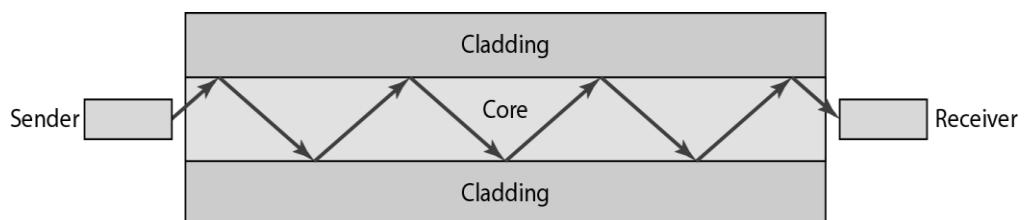
- Light travels in a straight line as long as it moves through a single uniform substance. If traveling through one substance suddenly enters another, ray changes its direction. (Refer fig 5.9)

### Bending of light ray



**Fig 5.9 – Bending of light ray**

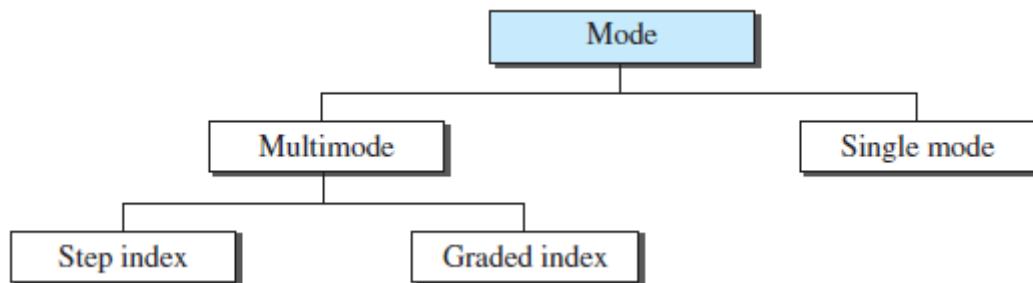
- If the angle of incidence (the angle the ray makes with the line perpendicular to the interface between the two medium) is less than the critical angle the ray refracts and move closer to the surface.
- If the angle of incidence is equal to the critical angle, the light bends along the interface.
- If the angle of incidence is greater than the critical angle, the ray reflects and travels again in the denser substance. Critical angle differs from one medium to another medium.
- Optical fiber use reflection to guide light through a channel. (Refer fig 5.10)



**Fig 5.10 – Core and cladding**

- A Glass or plastic core is surrounded by a cladding of less dense glass or plastic.

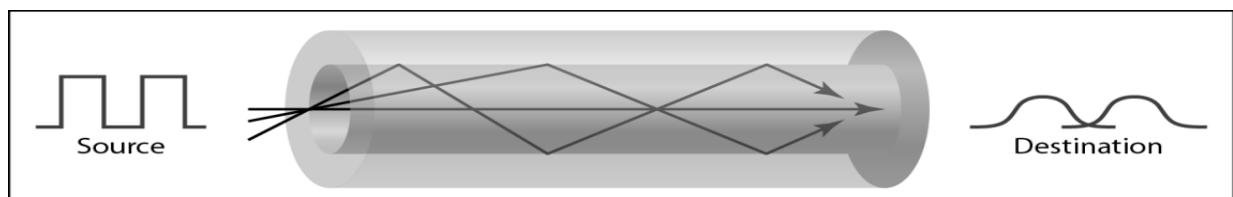
### Propagation Modes



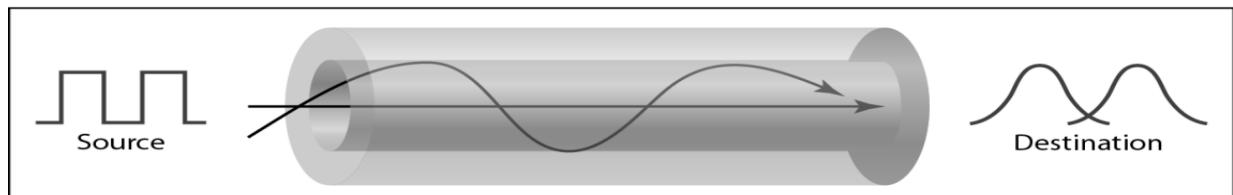
**Fig 5.11 – Propagation modes**

### Multimode

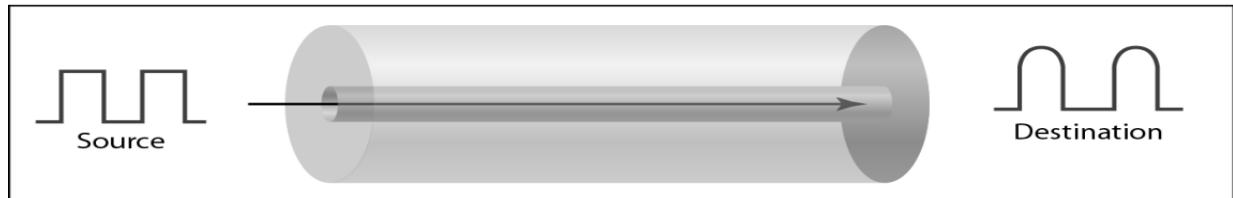
- In the multiple mode, multiple light beams from a source move through the core in different paths. (Refer fig 5.11 and 5.12)
- **Multimode-Step-Index fiber:** The density of core remains constant from the Centre to the edge.
- A ray of light moves through this constant density in a straight line until it reaches the interface of the core and the cladding. At the interface there is an abrupt change to a lower density that changes the angle of the beam's motion.
- **Multimode- Graded -Index fiber:** The density is varying. Density is highest at the centre of the core and decreases gradually to its lowest at the edge.



a. Multimode, step index



b. Multimode, graded index



c. Single mode

**Fig 5.12 – Multimode and single mode****Single Mode**

- Single mode uses step-index fiber and a highly focused source of light that limits beams to a small range of angles, all close to the horizontal.
- The single mode fiber itself is manufactured with a much smaller diameter than that of multimedia fiber.

**Connectors**

- **Subscriber channel (SC) connector** is used for cable TV.
- **Straight-tip (ST) connector** is used for connecting cable to networking devices.

**Advantages of Optical Fiber**

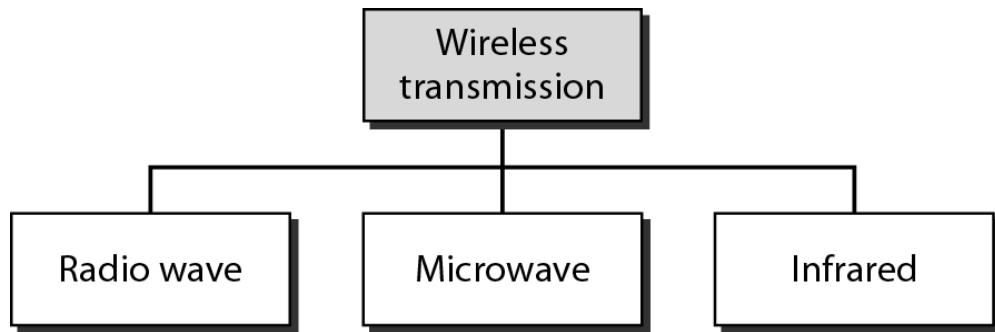
- Noise resistance
- Less signal attenuation
- Light weight

**Disadvantages**

- Cost
- Installation and maintenance
- Unidirectional
- Fragility (easily broken)

**Unguided media**

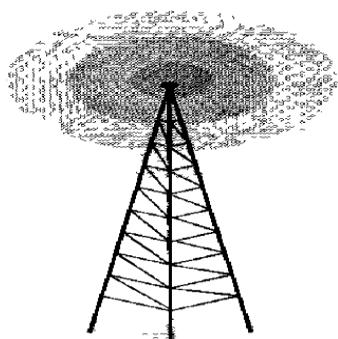
- Unguided media transport electromagnetic waves without using a physical conductor.
  - This type of communication is often referred to as wireless communication.
  - Signals are normally broadcast through air and thus available to anyone who has device capable of receiving them. (Refer fig 5.13)
- Unguided signals can travel from the source to destination in several ways:
- **Ground propagation** – waves travel through lowest portion on atmosphere.
  - **Sky propagation** – High frequency waves radiate upward into ionosphere and reflected back to earth.
  - **Line-of-sight propagation** – Very high frequency signals travel in a straight line.

**Fig 5.13 – Wireless Transmission****Radio Waves**

- Electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called radio waves.

**Properties**

- Radio waves are omnidirectional. When an antenna transmits radio waves, they are propagated in all directions. This means that the sending and receiving antennas do not have to be aligned. (Refer fig 5.14)
- A sending antenna sends waves that can be received by any receiving antenna.
- Radio waves, particularly those of low and medium frequencies, can penetrate walls.

**Fig 5.14 – Omnidirectional antenna****Disadvantages**

- The omnidirectional property has a disadvantage, that the radio waves transmitted by one antenna are susceptible to interference by another antenna that may send signals using the same frequency or band.
- As Radio waves can penetrate through walls, we cannot isolate a communication to just inside or outside a building.

**Applications**

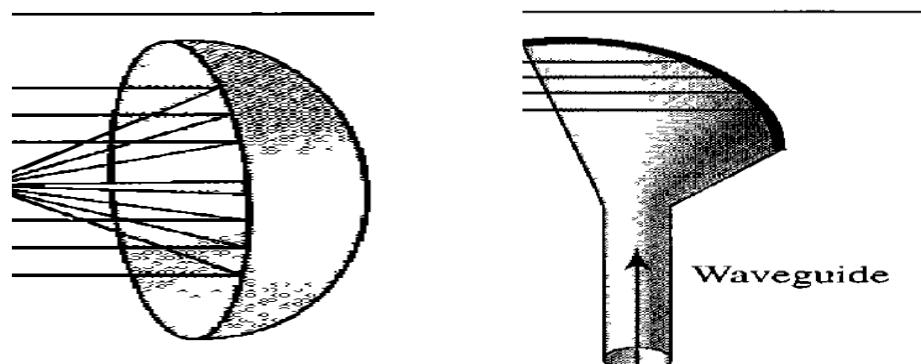
- Radio waves are used for multicast communications, such as radio and television, and paging systems.

**Microwaves**

- Electromagnetic waves having frequencies between 1 and 300 GHz are called microwaves. (Refer fig 5.15)

**Properties**

- Microwaves are unidirectional.
- Sending and receiving antennas need to be aligned.
- Microwave propagation is line-of-sight.
- Very high-frequency microwaves cannot penetrate walls.



**Fig 5.15 – a) Parabolic Dish antenna, b) Horn antenna**

- Parabolic Dish antenna focus all incoming waves into single point.
- Outgoing transmissions are broadcast through a horn aimed at the dish.

**Disadvantage**

- If receivers are inside buildings, they cannot receive these waves

**Applications**

- Microwaves are used for unicast communication such as cellular telephones, satellite networks, and wireless LANs.

**Infrared**

- Electromagnetic waves with frequencies from 300 GHz to 400 THz are called infrared rays.
- Infrared waves, having high frequencies, cannot penetrate walls.

**Applications**

- Infrared signals can be used for short-range communication in a closed area using line-of-sight propagation.

#### 4. Discuss Media Access Layer Protocols in detail.

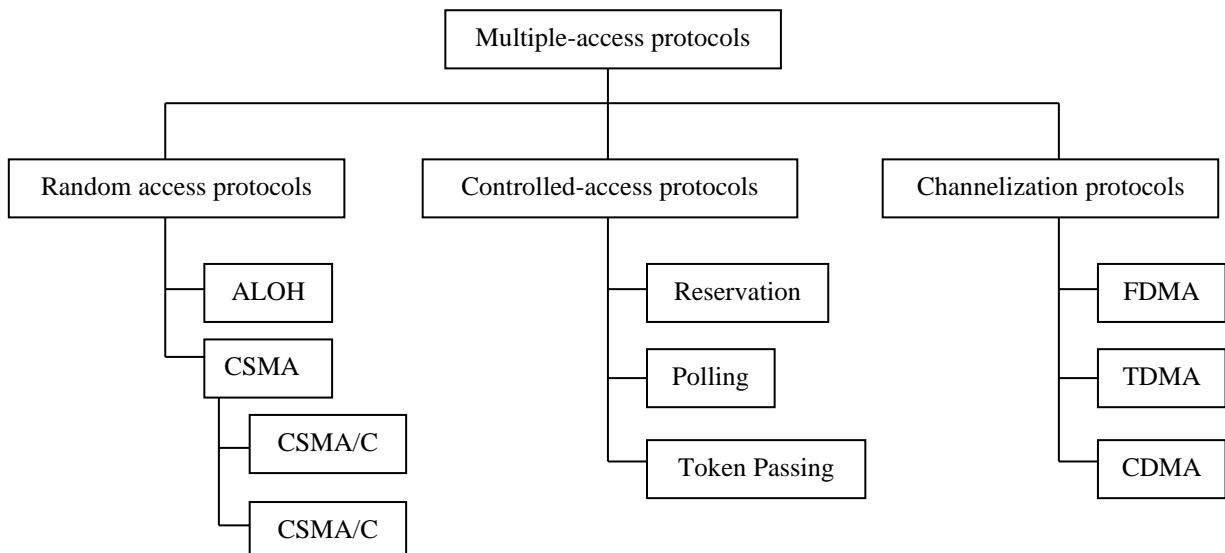
##### Synopsis:

- **Definition**
- **Taxonomy of multiple access protocols**
- **Random access**
  - **Two Features of Random Access**
- **CSMA**
- **Vulnerable Time**
- **Persistence Methods**
- 

##### **Definition**

- When nodes or stations are connected and use a common link, called a multipoint or broadcast link, we need a multiple-access protocol to coordinate access to the link.(Refer Flow chart 5.1)

##### **Taxonomy of multiple access protocols**



**Flow chart 5.1**

##### **Random access**

- In random access or contention methods, no station is superior to another station and none is assigned to control over another.
- No station permits, or does not permit another station to send.

## Two Features of Random Access

- There is no scheduled time for a station to transmit as the name implies. No rules specify which station should send next.
- Stations fight with one another to access the medium by a method called contention methods.

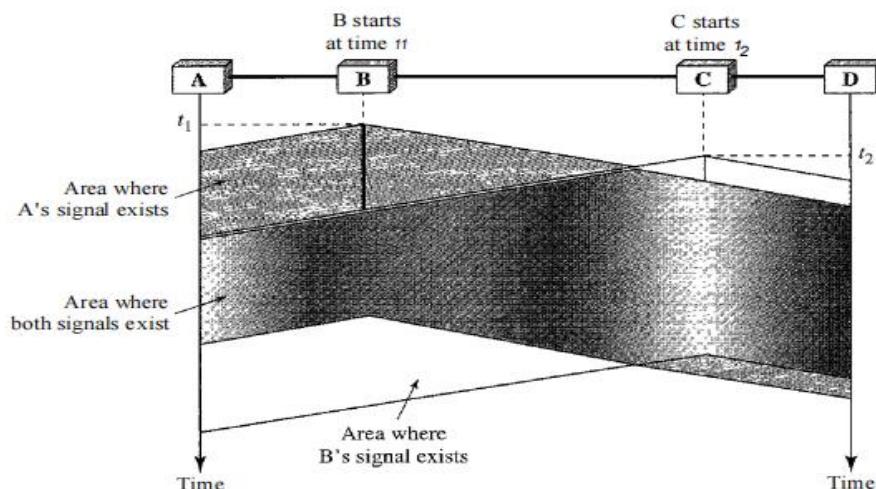
### CSMA - Carrier Sense Multiple Access

#### CD - Collision Detection

#### CA - Collision Avoidance

### CSMA:NOV/DEC 2023

- To minimize the chance of collision and increase the performance CSMA method was developed.
- The chance of collision can be reduced if a station senses the medium before trying to use it.
- Carrier sense multiple access (CSMA) requires that each station first listen to the medium (or check the state of the medium) before sending.
- In other words, CSMA is based on the principle “sense before transmit” or “listen before talk. (Refer fig 5.16)
- CSMA can reduce the possibility of collision, but it cannot eliminate it.



**Fig 5.16 – CSMA**

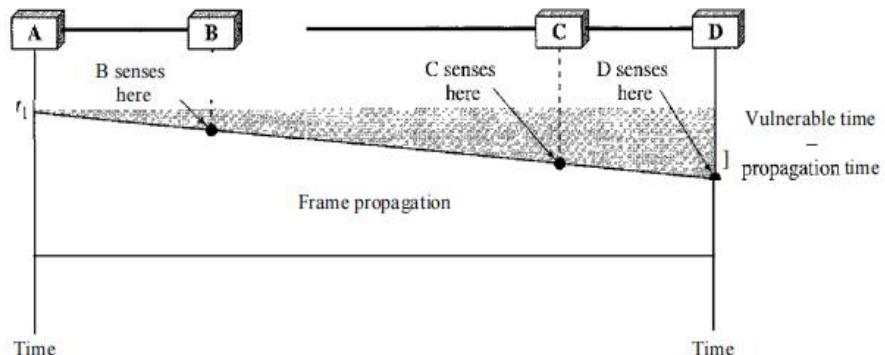
### Space/time model of the collision in CSMA

- At time  $t_1$ , station B senses the medium and finds it idle, so it sends a frame.
- At time  $t_2$  ( $t_2 > t_1$ ), station C senses the medium and finds it idle because, at this time, the first bits from station B have not reached station C.
- Station C also sends a frame.

- The two signals collide and both frames are destroyed.

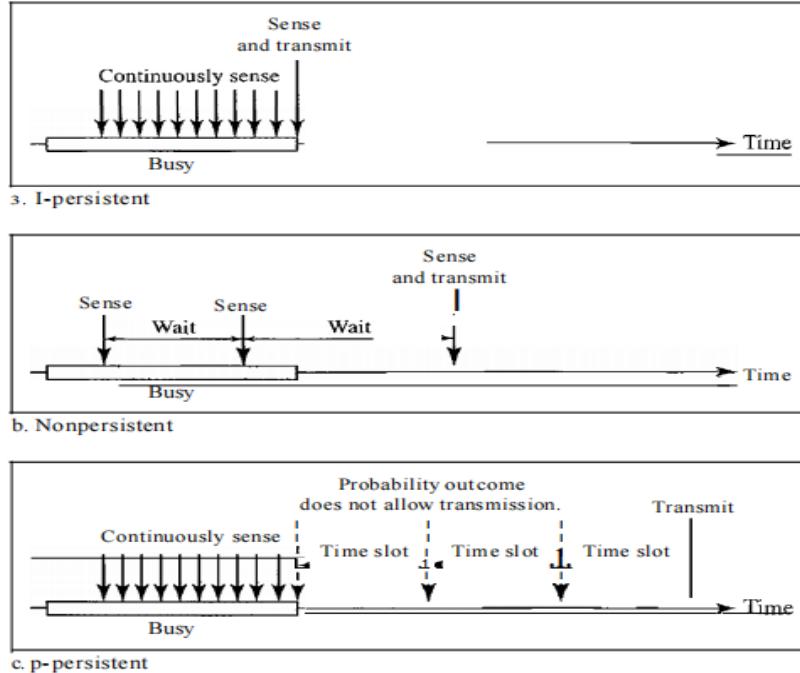
### Vulnerable Time

- The vulnerable time for CSMA is the propagation time  $T_p$ .
- This is the time 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 a frame during this time, a collision will result. (Refer fig 5.17)



**Fig 5.17 – Vulnerable Time**

### Persistence Methods



**Fig 5.18 – Persistence Methods**

**Behavior of three persistence methods****1-Persistent:**

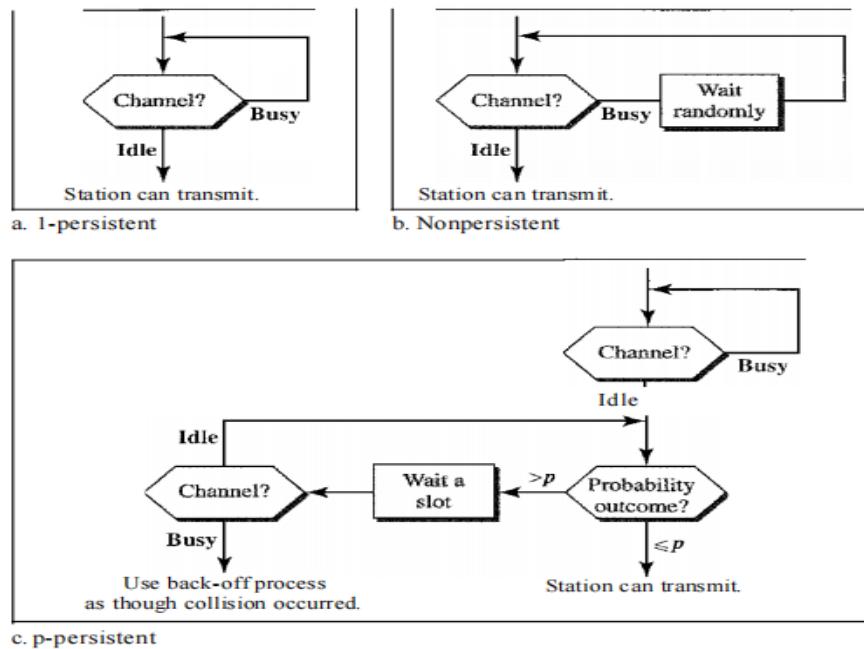
- The 1-persistent method is simple and straightforward.
- In this method, after the station finds the line idle, it sends its frame immediately (with probability 1).
- This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately. (Refer fig 5.18)

**Nonpersistent:**

- In the nonpersistent method, a station that has a frame to send senses the line.
- If the line is idle, it sends immediately.
- If the line is not idle, it waits a random amount of time and then senses the line again.
- The nonpersistent approach reduces the chance of collision because it is unlikely that two or more stations will wait the same amount of time and retry to send simultaneously.

**P-Persistent:**

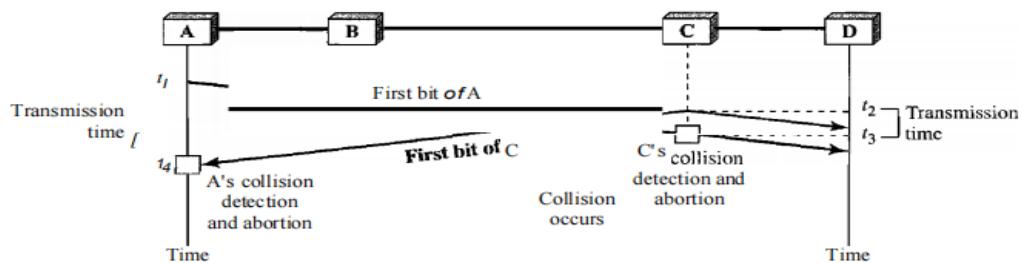
- The p-persistent method is used if the channel has time slots with slot duration equal to or greater than the maximum propagation time.
  - The p-persistent approach combines the advantages of the other two strategies.
  - It reduces the chance of collision and improves efficiency.
- In this method, after the station finds the line idle it follows these steps: (Refer fig 5.20)
- ✓ With probability  $p$ , the station sends its frame.
  - ✓ With probability  $q=1-p$ , the station waits for the beginning of the next time slot and checks the line again.
    - If the line is idle, it goes to step 1.
    - If the line is busy, it acts as though a collision has occurred and uses the backoff procedure.

**Fig 5.19 – Persistence Methods behavior**

- CSMA/CD tells the station what to do when a collision is detected. CSMA/CA tries to avoid the collision.

#### Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

- Carrier sense multiple access with collision detection (CSMA/CD) augments the algorithm to handle the collision. (Refer fig 5.20)
- A station monitors the medium after it sends a frame to see if the transmission was successful.
- If so, the station is finished. If, however, there is a collision, the frame is sent again.

**Fig 5.20 – CSMA/CD**

- Collision of the first bit in CSMA/CD
- At time  $t_1$ , station A has executed its persistence procedure and starts sending the bits of its frame.

- At time  $t_2$ , station C has not yet sensed the first bit sent by A.
- Station C executes its persistence procedure and starts sending the bits in its frame, which propagate both to the left and to the right.
- The collision occurs sometime after time  $t_2$ .
- Station C detects a collision at time  $t_3$  when it receives the first bit of A's frame.
- Station C immediately (or after a short time, but we assume immediately) aborts transmission.
- Station A detects collision at time  $t_4$  when it receives the first bit of C's frame; it also immediately aborts transmission.
- Looking at the figure, we can see that A transmits for the duration  $t_4 - t_1$ ; C transmits for the duration  $t_3 - t_2$ .

**Minimum Frame Size:**

- For CSMA/CD to work, we need a restriction on the frame size.
- Before sending the last bit of the frame, the sending station must detect a collision, if any, and abort the transmission.
- This is so because the station, once the entire frame is sent, does not keep a copy of the frame and does not monitor the line for collision detection. Therefore, the frame transmission time  $T_{ff}$  must be at least two times the maximum propagation time  $T_p$ .

**Example**

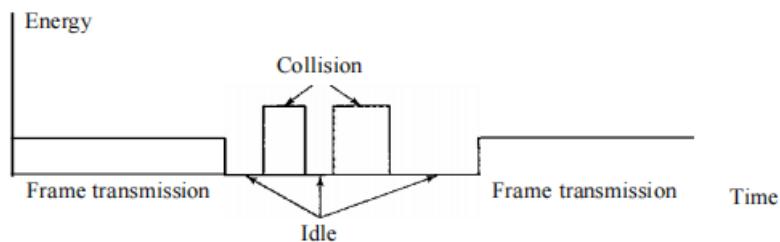
A network using CSMA/CD has a bandwidth of 10 Mbps. If the maximum propagation time (including the delays in the devices and ignoring the time needed to send a jamming signal) is  $25.6\mu s$ , what is the minimum size of the frame?

**Solution:** The frame transmission time is  $T_{ff} = 2 \times T_p = 51.2\mu s$ . This means, in the worst case, a station needs to transmit for a period of  $51.2\mu s$  to detect the collision. The minimum size of the frame is  $10 \text{ Mbps} \times 51.2\mu s = 512 \text{ bits or } 64 \text{ bytes}$ .

**Energy Level:**

- Level of energy in a channel can have three values: Zero, normal, and abnormal. (Refer fig 5.21)
- At the zero level, the channel is idle.
- At the normal level, a station has successfully captured the channel and is sending its frame.
- At the abnormal level, there is a collision and the level of the energy is twice the normal level.

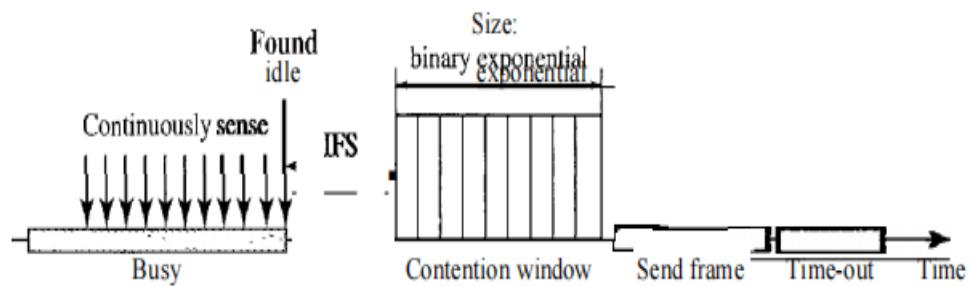
- A station that has a frame to send or is sending a frame needs to monitor the energy level to determine if the channel is idle, bust or in collision mode.



**Fig 5.21 - Energy level during transmission, idleness or collision**

#### **Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)**

- The basic idea behind CSMA/CA is that a station needs to be able to receive while transmitting to detect a collision. (Refer fig 5.22)
- When there is no collision, the station receives one signal: its own signal.
- When there is a collision, the station receives two signals: its own signal and the signal transmitted by a second station.
- In a wired network, the received signal has almost the same energy as the sent signal because either the length of the cable is short or there are repeaters that amplify the energy between the sender and the receiver.
- This means that in a collision, the detected energy almost doubles.
- In a wireless network, much of the sent energy is lost in transmission.
- The received signal has very little energy.
- Therefore, a collision may add only 5 to 10 percent additional energy.
- This is not useful for effective collision detection.
- To avoid collisions on wireless networks because they cannot be detected carrier sense multiple access with collision avoidance (CSMA/CA) was invented for this network.
- Collisions are avoided through the use of CSMA/CA's three strategies: the inter-frame space, the contention window, and acknowledgements.

**Fig 5.22 - Timing in CSMA/CA*****Inter-frame Space (IFS):***

- First, collisions are avoided by deferring transmission even if the channel is found idle.
- When an idle channel is found; the station does not send immediately.
- It waits for a period of time called the inter-frame space or IFS.
- Even though the channel may appear idle when it is sensed, a distant station may have already started transmitting.
- The distant station's signal has not yet reached this station.
- The IFS time allows the front of the transmitted signal by the distant station to reach this station.
- If after the IFS time the channel is still idle, the station can send, but it still needs to wait a time equal to the contention time.
- In CSMA/CA, the IFS can also be used to define the priority of a station or a frame.

***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.
- This means that it is set to one slot the first time and then doubles each time the station cannot detect an idle channel after the IFS time.
- The contention window is that the station needs to sense the channel after each time slot.
- In CSMA/CA, if the station finds the channel busy, it does not restart the timer of the contention window; it stops the timer and restarts it when the channel becomes idle.

### Acknowledgment

- With all these precautions, there still may be a collision resulting in destroyed data.
- In addition, the data may be corrupted during the transmission.
- The positive acknowledgment and the time-out timer can help guarantee that the receiver has received the frame.

### NOTE

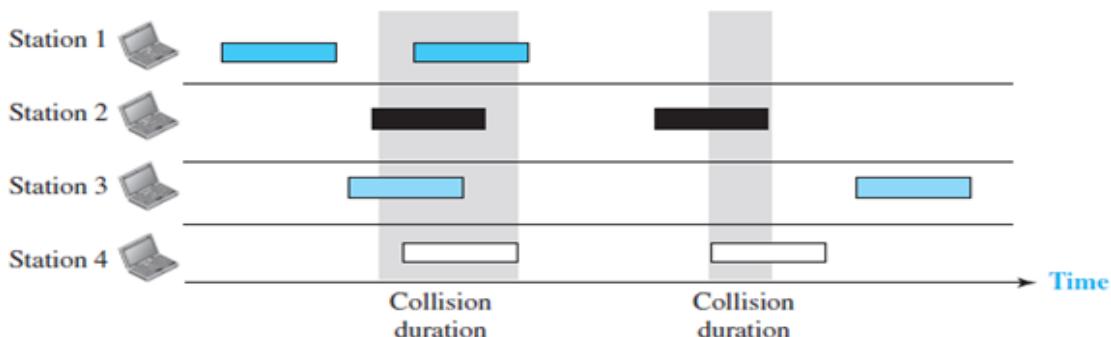
Exponential backoff:

The strategy of doubling the delay interval between each retransmission attempt is a general technique known as **exponential backoff**.

### ALOHA

#### ➤ Pure ALOHA

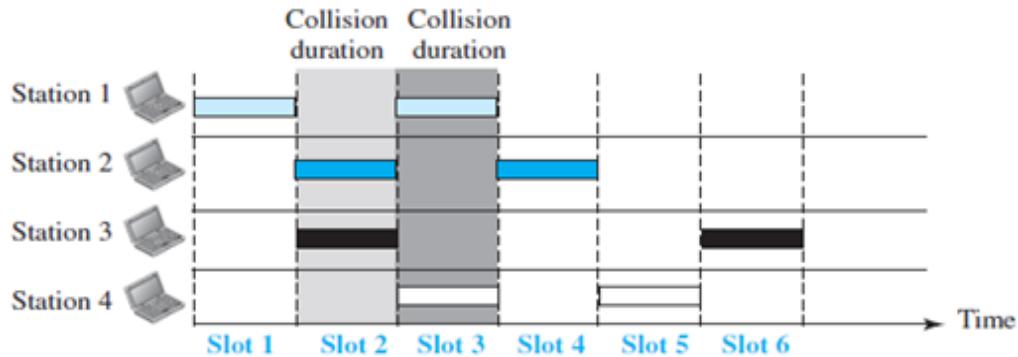
- The original ALOHA protocol is called ***pure ALOHA***.
- This is a simple but elegant protocol. The idea is that each station sends a frame whenever it has a frame to send (multiple access).
- However, since there is only one channel to share, there is the possibility of collision between frames from different stations. Figure 5.23 shows an example of frame collisions in pure ALOHA.



**Fig 5.23 – Frames in a pure ALOHA network**

#### ➤ Slotted ALOHA

- Pure ALOHA has a vulnerable time of  $2 * T_{fr}$ . This is so because there is no rule that defines when the station can send.
- A station may send soon after another station has started or just before another station has finished. Slotted ALOHA was invented to improve the efficiency of pure ALOHA.
- In **slotted ALOHA** we divide the time into slots of  $T_{fr}$  seconds and force the station to send only at the beginning of the time slot. Figure 5.24 shows an example of frame collisions in slotted ALOHA.



**Fig 5.24 – Frames in a slotted ALOHA network**

**5. Explain in detail about wired LAN - Ethernet (IEEE 802.3) and its frame format (OR)  
Explain the physical properties of Ethernet 802.3 with necessary diagram (NOV 2014)**

(May, Nov 2015 & 2016).

**Synopsis:**

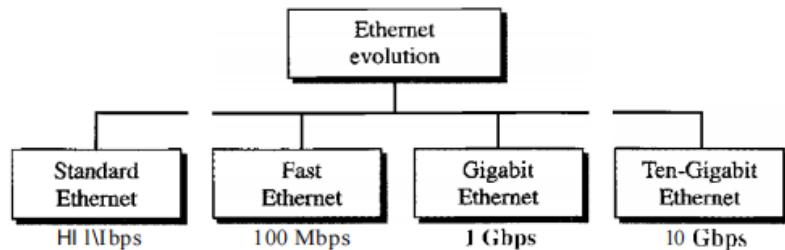
- **Introduction**
- **Ethernet Evolution**
- **Physical properties**
- **Transmitter algorithm**

**Introduction:**

- The IEEE 802.3 standards committee developed a widely used LAN standard called Ethernet, which covers both the MAC layer and the physical layer. (Refer fig 5.25)
- The Ethernet is a multiple-access network, meaning that a set of nodes send and receive frames over a shared link.
- The IEEE 802.3 standard uses CSMA for controlling media access and the 1-persistent algorithm explained earlier, although the lost time owing to collisions is very small.
- Also, IEEE 802.3 uses a back-off scheme known as binary exponential backoff.
- The use of random backoff minimizes subsequent collisions.
- This back-off scheme requires a random delay to be doubled after each retransmission.
- The user drops the frame after 16 retries.
- The combination of the 1-persistent scheme and binary exponential backoff results in an efficient scheme.
- The Ethernet versions have different data rates.

- Version 1000BaseSX, carrying 1 Gb/s, and 10GBase-T, carrying 10 Gb/s, hold the most promise for the future of high-speed LAN development.

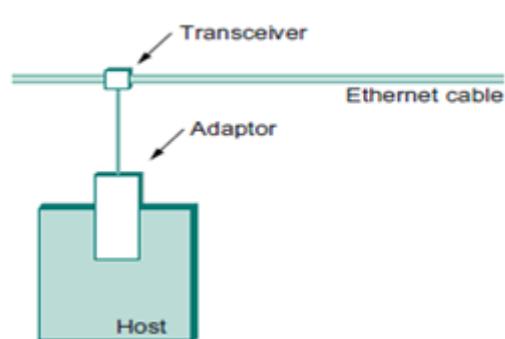
### Ethernet Evolution



**Fig 5.25 – Ethernet evolution**

### Physical properties:

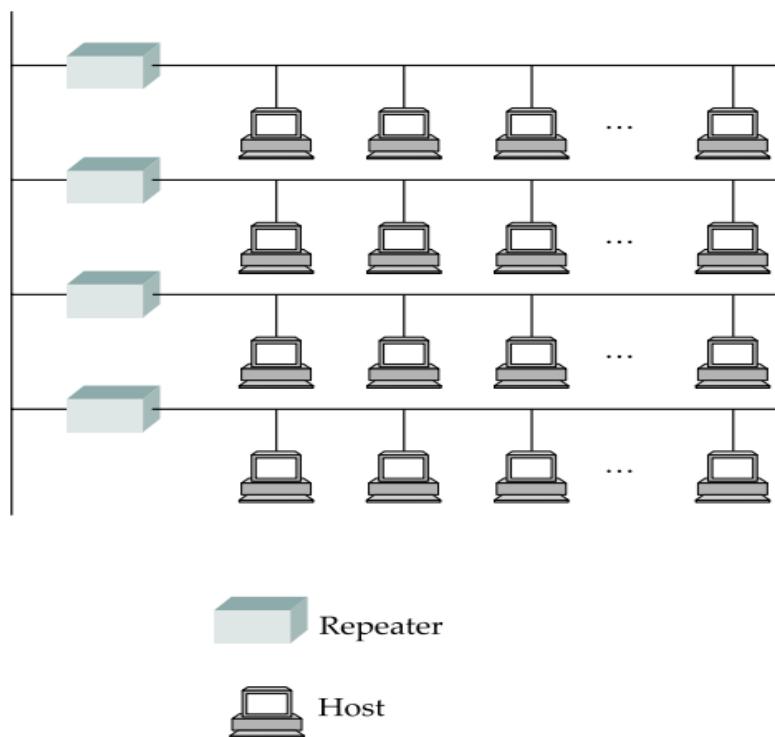
- An Ethernet segment is implemented on a coaxial cable of up to 500m.
- This cable is similar to the type used for cable TV, except that it typically has an impedance of 50 ohms instead of cable TV's 75 ohms. (Refer fig 5.26)
- Hosts connect to an Ethernet segment by tapping into it; taps must be at least 2.5 m apart.
- A transceiver – a small device directly attached to the tap – detects when the line is idle and drives the signal when the host is transmitting.
- It also receives incoming signals.



**Fig 5.26 – Ethernet transceiver and adoptor**

- The transceiver is, in turn, connected to an Ethernet adaptor, which is plugged into the host.
- Multiple Ethernet segments can be joined together by repeaters.
- A repeater is a device that forwards digital signals, much like an amplifier forwards analog signals.

- However, no more than four repeaters may be positioned between any pair of hosts, meaning that an Ethernet has a total reach of only 2,500 m.
- Rather than using a 50-ohm coax cable, an Ethernet can be constructed from a thinner cable known as 10Base2; the original cable is called 10Base5 (the two cables are commonly called thin-net and thick-net, respectively).
- The “10” in 10Base2 means that the network operates at 10 Mbps, “Base” refers to the fact that the cable is used in a baseband system, and the “2” means that a given segment can be no longer than 200 m.
- Today, a third cable technology is predominantly used, called 10BaseT, where the “T” stands for twisted pair. (Refer fig 5.27 and 28)
- A 10BaseT segment is usually limited to less than 100 m in length.
- Data transmitted by any one host on the Ethernet reaches all the other hosts.
- This is the good news.
- The bad news is that all these hosts are competing for access to the same link, and as a consequence, they are said to be in the same collision domain.



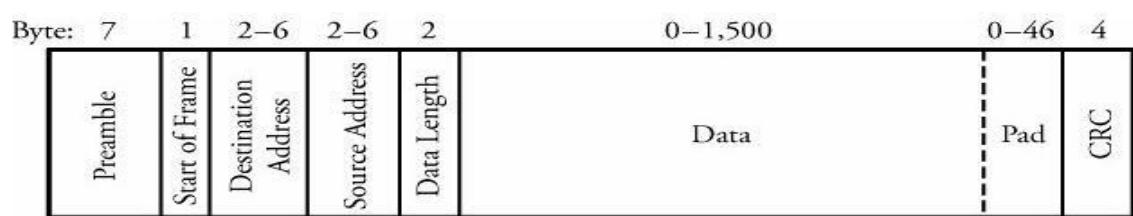
**Fig 5.27 – Ethernet repeater**

**Fig 5.28 – Ethernet hub****Access Protocol:**

- The algorithm that controls access to the shared Ethernet link.
- This algorithm is commonly called the Ethernet's media access control (MAC). It is typically implemented in hardware on the network adaptor.

**Frame Format:**

- A brief description of the frame fields follows and is shown in the below figure. (Refer fig 5.29)
  - **Preamble** is 7 bytes and consists of a pattern of alternating 0s and 1s. This field is used to provide bit synchronization.
  - **Start of frame** consists of a 10101011 pattern and indicates the start of the frame to the receiver.
  - **Destination address** specifies the destination MAC address.
  - **Source address** specifies the source MAC address.
  - **Length/Type** specifies the frame size, in bytes. The maximum Ethernet frame size is 1,518 bytes.
  - **LLC** data is data from the LLC layer.
  - **Pad** is used to increase the frame length to the value required for collision detection to work.
  - Frame check sequence is 32-bit CRC for error checking.

**Fig 5.29 – Ethernet IEEE 802.3 LAN frame**

### **Address**

- Each host on an Ethernet – has a **unique Ethernet address**.
- Ethernet addresses are typically printed in a form humans can read as a sequence of six numbers separated by colons.
- Each number corresponds to 1 byte of the 6-byte address and is given by a pair of hexadecimal digits, one for each of the 4-bit nibbles in the byte; leading 0s are dropped.
- For example, 8:0:2b:e4:b1:2 is the human-readable representation of Ethernet address as follows,

00001000 00000000 00101011 11100100 10110001 00000010

- Each frame transmitted on an Ethernet is received by every **adaptor** connected to that Ethernet.
- Each **adaptor** recognizes those frames addressed to its address and passes only those frames on to the host.

### **An Ethernet adaptor receives all frames and accepts**

- Frames addressed to its own address
- Frames addressed to the broadcast address
- Frames addressed to a multicast address, if it has been instructed to listen to that address
- All frames, if it has been placed in promiscuous mode.
- It passes to the host only the frames that it accepts.

### **Transmitter algorithm:**

#### **1-Persistent:**

- The 1-persistent method is simple and straightforward.
- In this method, after the station finds the line idle, it sends its frame immediately (with probability 1).
- This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately.

#### **P-Persistent:**

- The p-persistent method is used if the channel has time slots with a slot duration equal to or greater than the maximum propagation time.
- The p-persistent approach combines the advantages of the other two strategies.
- It reduces the chance of collision and improves efficiency.

In this method, after the station finds the line idle it follows these steps:

- With probability  $p$ , the station sends its frame.
- With probability  $q=1-p$ , the station waits for the beginning of the next time slot and checks the line again.
  - ✓ If the line is idle, it goes to step 1.
  - ✓ If the line is busy, it acts as though a collision has occurred and uses the backoff procedure.

**6. Discuss the functioning (Key requirements) of wireless LAN in detail. (May 2015, Nov 2015) May 2016.(NOV/DEC 2023),(April/may 2024)**

**Synopsis:**

- **Introduction**
- **Architecture**
- **Station Types**

**Introduction**

- Wireless technologies differ from wired links in some important ways, while at the same time sharing many common properties.
- Like wired links, issues of bit errors are of great concern—typically even more so due to the unpredictable noise environment of most wireless links. Framing and reliability also have to be addressed.
- Unlike wired links, power is a big issue for wireless, especially because wireless links are often used by small mobile devices (like phones and sensors) that have limited access to power (e.g., a small battery).
- Furthermore, you can't go blasting away at arbitrarily high power with a radio transmitter—there are concerns about interference with other devices and usually regulations about how much power a device may emit at any given frequency. (Refer table 5.2)

	Bluetooth (802.15.1)	Wi-Fi (802.11)	3G Cellular
Typical link length	10 m	100 m	Tens of kilometers
Typical data rate	2 Mbps (shared)	54 Mbps (shared)	Hundreds of kbps (per connection)
Typical use	Link a peripheral to a computer	Link a computer to a wired base	Link a mobile phone to a wired tower
Wired technology analogy	USB	Ethernet	DSL

**Table 5.2 – Wireless LAN types**

**Introduction** IEEE has defined the specification for the wireless LAN called IEEE 802.11, which covers the physical and Data Link Layers.

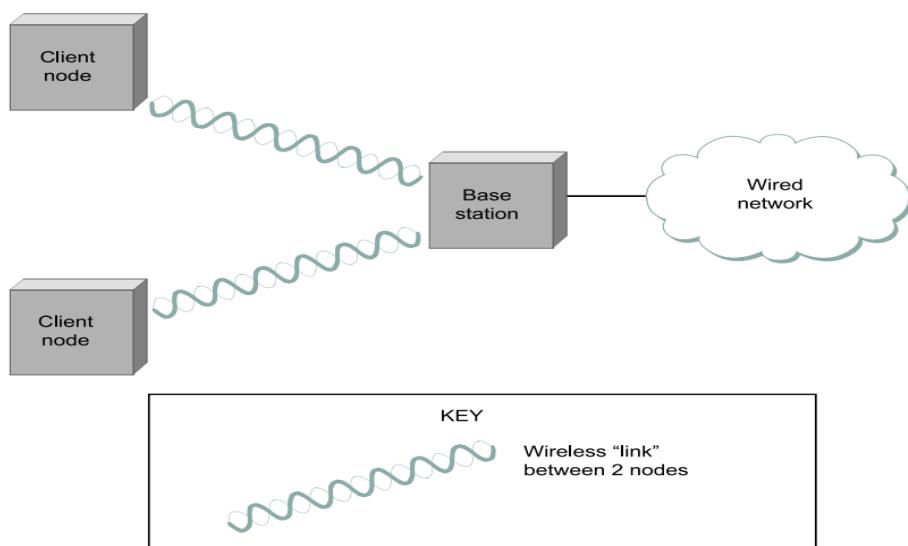
### Architecture

IEEE 802.11 standard defines 2 kinds of services.

1. The basic service set (BSS)
2. The extended service set (ESS)

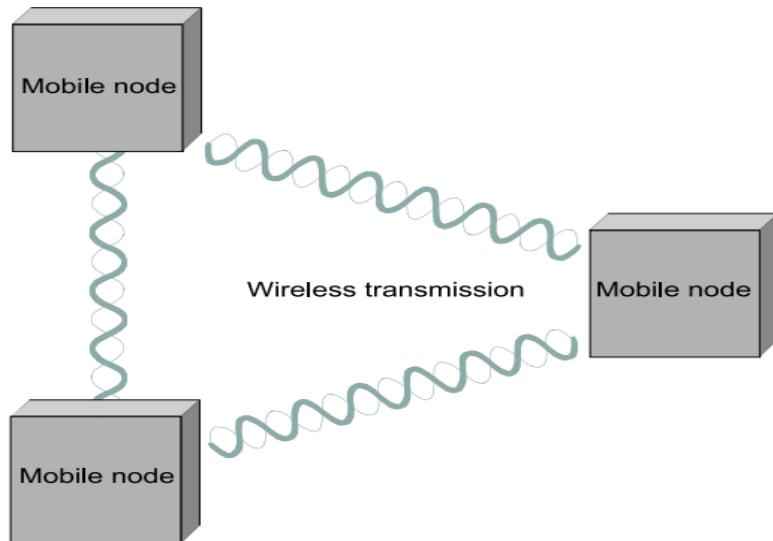
#### **1) Basic Service Set (BSS):**

A BSS is made of stationary (immobile) or mobile wireless stations and a possible central base station known as the access point AP. (Refer fig 5.30)

**Fig 5.30 – BSS – central base station**

### **Mesh or ad hoc network**

The BSS without an AP is stand alone network and cannot send data to other BSS. It is called an ad hoc architecture (Refer fig 5.31)



**Fig 5.31 – BSS – ad hoc network**

### **2) Extended Service Set (ESS):**

- An ESS is made up of two or more BSS with AP. The BSS are connected through a distribution system, which is usually a wired LAN.
- An ESS uses two types of stations mobile and stationary.
- The mobile stations are normal stations inside a BSS.
- The stationary stations are AP stations that are part of the wired LAN. When BSS are connected, the network is called an infrastructure network.
- In this the stations within reach of one another can communicate without the use of an AP. But communication between two stations in two different BSS usually occurs via two AP's.

### **Station Types**

Three qualitatively different levels of mobility in a wireless LAN.

1. No transmission
2. BSS transition
3. ESS transition

**1) No transmission:**

The first level is no mobility, such as when a receiver must be in a fixed location to receive a directional transmission from the base station of a single BSS.

**2) BSS transition:**

It is defined as a station movement from one BSS to another BSS within the same ESS (Bluetooth).

**3) ESS transition**

It is defined as a station movement from a BSS in one ESS to a BSS with in another ESS. The third level is mobility between bases, as is the case with cell phones and Wi-Fi.

**7. Discuss IEEE 802.11 (or) WI-FI in detail (or) MAC layer functions in IEEE802.11 (May 2015, 2016, 2017)(Dec 2017).****Synopsis:**

- **Introduction**
- **Physical properties**
- **Protocol Stack**
- **IEEE 802.11 MAC Layer (May 2015)**
- **MACAW (NOV/DEC 2014)**
- **Distribution system**
- **MAC Frame**

**Introduction:**

- 802.11 is designed for use in a limited geographical area (homes, office buildings, campuses), and its primary challenge is to mediate access to a shared communication medium—in this case, signals propagating through space.

**Physical properties**

- IEEE 802.11 defines the specification for the conversion of bits to a signal in the physical layer.
- The IEEE 802.11 physical layer is of four types. (Refer fig 5.32).

### 1. Frequency-hopping spread spectrum (FHSS):

- It is a method in which the sender sends one carrier frequency for a short amount of time, and then hops to another carrier frequency for the same amount of time, hops again to still another same amount of time and so on.
- This technique makes use of 79 channels.
- FHSS operates in the 2.4 GHz ISM band and supports data rates of 1 Mb/s to 2 Mb/s.
  1. If the band width of the original signal is  $B$ , the allocated spread spectrum bandwidth is  $N \times B$ .
  2. The amount of time spent at each sub band is called the dwell time.

### 2. Direct-sequence spread spectrum (DSSS):

- It uses seven channels, each supporting data rates of 1 Mb/s to 2 Mb/s. The operating frequency range is 2.4 GHz ISM band.
- In DSSS each bit by the sender is replaced by the sequence of bits called chip code.
- To avoid buffering, the time needed to send one chip code must be the same as the time needed to send one original bit.

### 3. IEEE 802.11a:

- Orthogonal frequency division multiplexing (OFDM): IEEE 802.11a uses OFDM, which uses 12 orthogonal channels in the 5 GHz range.
- All the sub bands are used by one source at a given time.
- The common data rates are 18 Mbps and 54 Mbps.

#### Protocol Stack

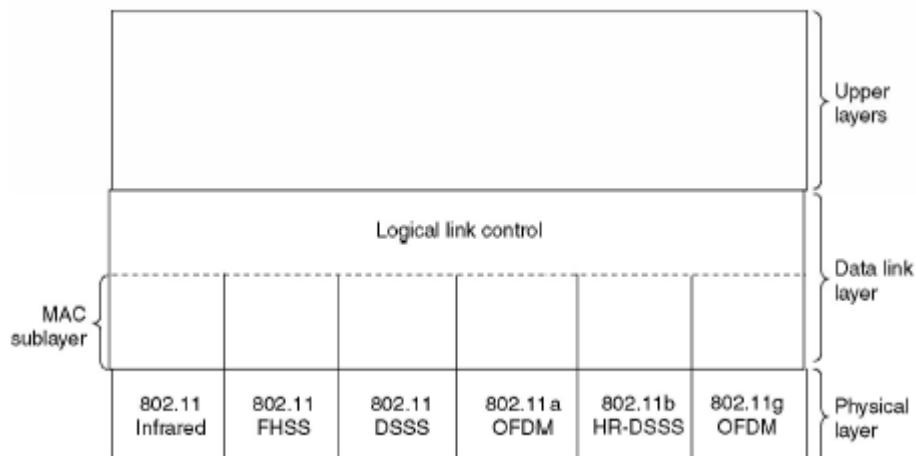


Fig 5.32 – IEEE802.11 protocol stack

**4. IEEE 802.11b:**

- High Rate Direct-Sequence spread spectrum (HRDSSS): IEEE 802.11b operates in the 2.4 GHz band and supports data rates of 5.5 Mb/s to 11 Mb/s.
- It is similar to DSSS except for the encoding method which is called complementary code keying (CCK).
- CCK encodes four or eight bits to one CCK symbol.

**5. IEEE 802.11g: (OFDM):**

- IEEE 802.11g operates at 2.4 GHz and supports even higher data rates.

**IEEE 802.11 MAC Layer (May 2015)**

- IEEE 802.11 provides several key functionalities: reliable data delivery, media access control, and security features.
- The MAC layer consists of two sub layers:
  1. The distributed-coordination function algorithm (DCF) and
  2. The point-coordination function algorithm (PCF).

**1) Point Coordination Function (PCF) Algorithm**

- The point-coordination function (PCF) provides a contention-free service.
- PCF is an optional feature in IEEE 802.11 and is built on top of the DCF layer to provide centralized media access.

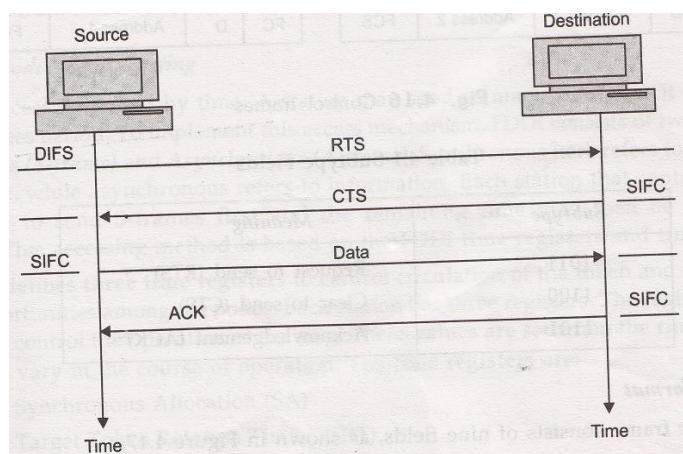
**2) Distributed Coordination Function (DCF) Algorithm**

- The DCF algorithm uses contention resolution, and its sublayer implements the CSMA scheme for media access control and contention resolution.
- Begin DCF Algorithm for Wireless 802.11 MAC – (Refer fig 5.33) **MACA (NOV/DEC 2014)**
  1. The sender senses the medium for any ongoing traffic.
  2. If the medium is idle, the sender waits for a time interval equal to IFS. Then the sender senses the medium again. If the medium is still idle, the sender transmits the frame immediately.

1. After the station is found ideal, the station waits for a period of time, called the distributed inter-frame space (DIFS).
2. The station sends a control frame called the request to send (RTS). After receiving the RTS and waiting a short period called the short inter-frame space (SIFS), the destination station sends a control frame called clear to send (CTS), to the source station. This control frame indicates that the destination station is ready to receive data.

Two or more stations made try to send RTS frames at the same time, these control frames may collide. The sender assumes there has been a collision if it has not received CTS frame from the receiver and it tries again.

3. The source station sends data after waiting an amount of time equal to SIFS.
4. The destination station after waiting for an amount of time equal to SIFS sends an acknowledgement to show that the frame has been received.
5. When a station sends an RTS frame, it includes the duration of the time that it needs to occupy the channel. The stations that are affected by this transmission create a timer called a Network Allocation Vector (NAV) that shows how much time must pass before these stations are allowed to check the channel for idleness.



**Fig 5.33 – RTS/CTS**

#### MACAW (NOV/DEC 2014)

WLAN data transmission collisions can still happen, and MACA for Wireless (MACAW) is brought to extend the functionality of MACA. It demands nodes to send

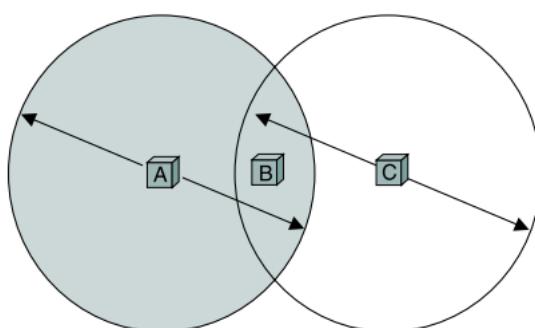
acknowledgments after every successful frame transmission. MACAW is commonly used in ad hoc networks. Moreover, it is the basis of various other MAC protocols found in wireless sensor networks (WSN).

### Collision Avoidance:

- ✓ **Hidden node problem**
- ✓ **Exposed node problem**

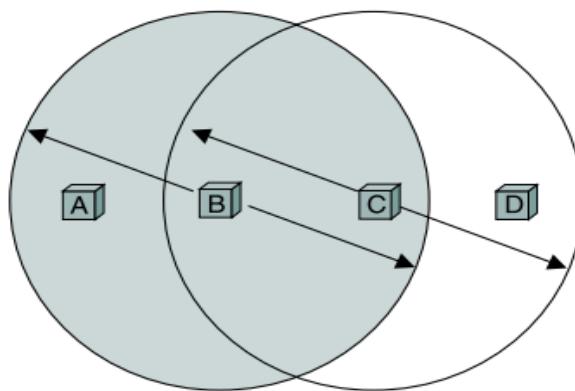
- A wireless protocol would follow the same algorithm as the Ethernet – wait until the link becomes idle before transmitting and back off should a collision occur – and to a first approximation, this is what 802.11 does.
- Consider the situation depicted in the below figure, where A and C are both within range of B but not each other.
- Suppose both A and C want to communicate with B and so they each send it a frame.
- A and C are unaware of each other since their signals do not carry that far.
- These two frames collide with each other at B, but unlike an Ethernet, neither A nor C is aware of this collision.
- A and C are said to be **hidden nodes** with respect to each other. (Refer fig 5.34)

**Note: The hidden node problem. Although A and C are hidden from each other, their signals can collide at B. (B's reach is not shown.)**



**Fig 5.34 – Hidden node problem**

- A related problem, called the **exposed node problem**, occurs under the circumstances illustrated in the below figure, where each of the four nodes is able to send and receive signals that reach just the nodes to its immediate left and right.
- For example, B can exchange frames with A and C but it cannot reach D, while C can reach B and D but not A. (Refer fig 5.35)

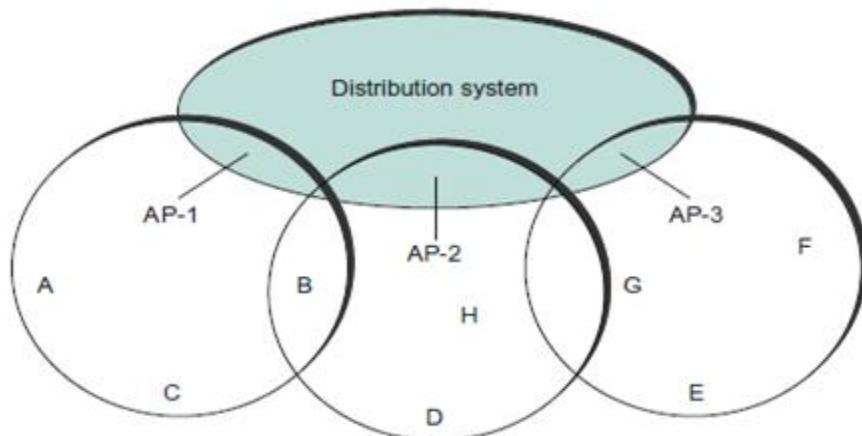


**Fig 5.35 – Exposed node problem**

**Note:** The exposed node problem. Although B and C are exposed to each other's signals, there is no interference if B transmits to A while C transmits to D. (A's and D's reaches are not shown.)

### Distribution system

- Some nodes are allowed to roam (e.g., your laptop) and some are connected to a wired network infrastructure.
- 802.11 calls these base stations access points (APs), and they are connected to each other by a so-called distribution system.
- Figure 5.36 illustrates a distribution system that connects three access points, each of which services the nodes in some region.
- Each access point operates on some channel in the appropriate frequency range, and each AP will typically be on a different channel than its neighbors.
- Although two nodes can communicate directly with each other if they are within reach of each other, the idea behind this configuration is that each node associates itself with one access point.
- For node A to communicate with node E, for example, A first sends a frame to its access point (AP-1), which forwards the frame across the distribution system to AP-3, which finally transmits the frame to E. How AP-1 knew to forward the message to AP-3 is beyond the scope of 802.11; it may have used the bridging protocol described in the next chapter (Section 3.1.4). What 802.11 does specify is how nodes select their access points and, more interestingly, how this algorithm works in light of nodes moving from one cell to another.

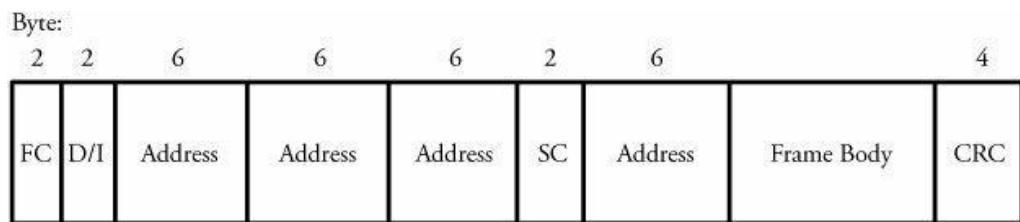
**Fig 5.36 – Distribution system**

The technique for selecting an AP is called *scanning* and involves the following four steps:

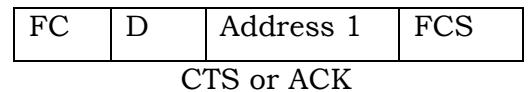
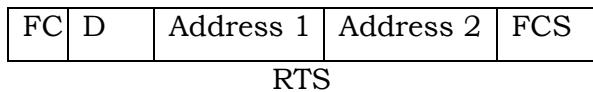
1. The node sends a Probe frame.
2. All APs within reach reply with a Probe Response frame.
3. The node selects one of the access points and sends that AP an Association Request frame.
4. The AP replies with an Association Response frame.

### **MAC Frame**

- The three frame types in IEEE 802.11 are control frames, data-carrying frames, and management frames.
- The frame format for the 802.11 MAC is shown in the below diagram and is described as follows. (Refer fig 5.37)
  - ✓ The frame control (FC) field provides information on the type of frame: control frame, data frame, or management frame.
  - ✓ Duration/connection ID (D/I) refers to the time allotted for the successful transmission of the frame.
  - ✓ The addresses field denotes the 6-byte source and destination address fields.
  - ✓ The sequence control (SC) field consists of 4 bits reserved for fragmentation and reassembly and 12 bits for a sequence number of frames between a particular transmitter and receiver.
  - ✓ The frame body field contains a MAC service data unit or control information.
  - ✓ The cyclic redundancy check (CRC) field is used for error detection.

**IEEE 802.11 MAC frame****Fig 5.37 – IEEE 802.11 MAC frame format**

- Control frames ensure reliable data delivery. The control frames are used for accessing the channel and acknowledgement frames. It consists of,



- Management frames are used to monitor and manage communication among various users in the IEEE 802.11 LAN through access points.

**7. Discuss in concepts of Packet Switched detail the Networks (Packet Switching).****Synopsis:**

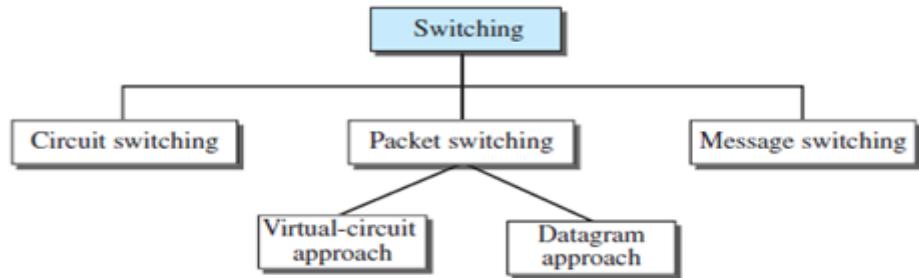
- **Introduction**
- **Switching**
- **Type of switching**
- **Packet switching**
- **Routing Table**
- **Virtual Circuit Approach**
- **Comparison between Virtual circuit and Datagram**
- **Virtual-Circuit Networks – characteristics**
- **Addressing**

**Introduction****Switching**

- To make communication among multiple devices efficiently, a process used is called switching.
- A switched network consists of a series of interlinked nodes called switches.

### Type of switching (Refer fig 5.38)

- Circuit Switching
- Packet Switching
- Message Switching



**Fig 5.38 – Taxonomy of switched networks**

### Advantages of packet switching over circuit switching are as follows:

- Circuit switching is suitable for **voice communication**. When circuit switched links are used for data transmission, the link is often idle and its facilities wasted.
  - The **data rate** of circuit switched connections for data transmission is very slow.
  - Circuit switching is **inflexible**. Once a circuit has been established, that the path taken by all parts of the transmission whether or not it remains the most efficient.
  - Circuit switching treats all transmission as equal. That means, there is no priority among the transmission of data.
- The mostly widely used switching technique for data transmission is *packet switching*.
- In this, the data are transmitted in the form of *packets*.
- If the length of the packet is too long then it is broken-up into multiple packets.
- Each packet contains data and also a header with control information.

### PACKET SWITCHING:

- There are two popular approaches to packet switching:
- Datagram approach and
  - Virtual circuit approach

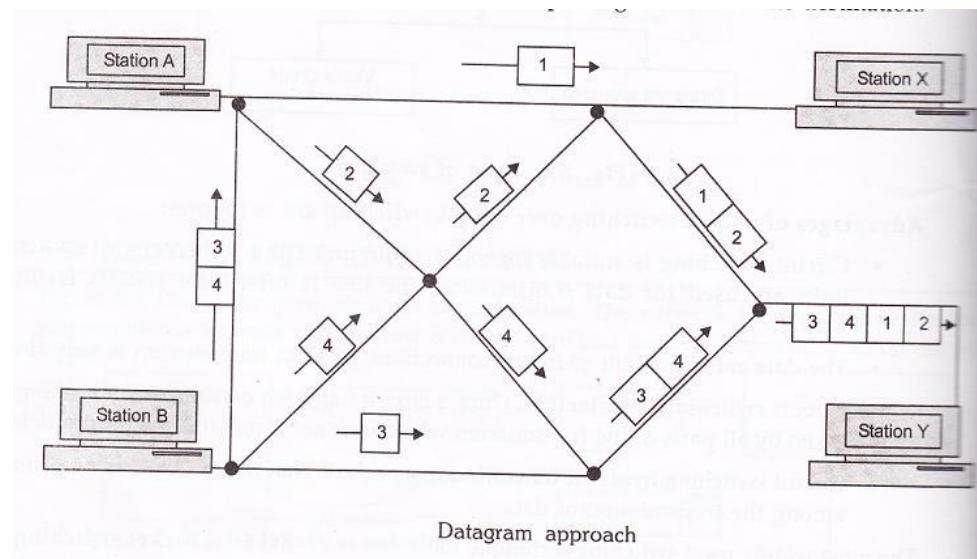
### Datagram Approach:

- In the datagram approach, each packet is treated independently from all others.
  - A datagram is a multipacket of the same message and it works on the principle of 'send' and 'forget'.
- The features of datagram are as follows:
- Circuit setup is not needed.
  - Each packet contains both source and destination address.
  - Each packet routed independently.
  - Few packets are lost during crash.

- No effect or router failure.

**Example:**

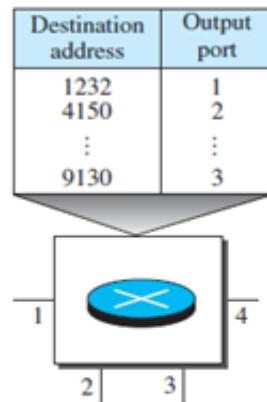
- The below figure shows how the datagram approach can be used to deliver four packets from station A to station Y. (Refer fig 5.39)
- In this example, all four packets belong to the same message but may go by different paths to reach their destination.
- This approach can cause the datagrams of a transmission to arrive at their destination out of order.
- In most protocols, it is the responsibility of transport layer to reorder the datagrams before passing them on to the destination.



**Fig 5.39– Datagram approach**

**Routing Table**

- In this type of network, each switch (or packet switch) has a routing table which is based on the destination address.
- The routing tables are dynamic and are updated periodically.
- The destination addresses and the corresponding forwarding output ports are recorded in the tables.
- This is different from the table of a circuit switched network (discussed later) in which each entry is created when the setup phase is completed and deleted when the teardown phase is over (Refer fig 5.40)



A switch in a datagram network uses a routing table that is based on the destination address.

**Fig 5.40 – Routing table in a datagram network**

#### **Virtual Circuit Approach:**

- In the virtual circuit approach, the relationship between all packets belonging to a message or session is preserved.
  - A single route is chosen between sender and receiver at the beginning of the session.
  - When the data are sent, all packets of the transmission travel one after another along that route.
- Virtual circuit transmission is implemented in two formats:
- Switched Virtual Circuit (SVC)
  - Permanent Virtual Circuit (PVC)

#### **Switched Virtual Circuit (SVC)**

- In the **switched virtual circuit (SVC)** method, a virtual circuit is created whenever it is needed exists only for the duration of the specific exchange.
- If the station A wants to send four packets to station X, first it requests the establishment of a connection to station X.
- Once the connection is established, the packets are sent one after another and in sequential order. When the last packet has been received, the connection is released and that virtual circuit ceases to exist.
- Only one single route exists for the duration of transmission. Each time that station A wants to communicate with station X, a new route is established.

### Permanent Virtual Circuit (PVC)

- In the **permanent Virtual Circuit (PVC)** method, the same virtual circuit is provided between two users on a continuous basis.
  - This circuit is dedicated to the specific users. No one else can use it, because it is always in place.
  - It can be used without connection establishment and connection termination.
- Two SVC users may get a different route every time they request a connection whereas two PVC users always get the same route.

### Comparison between Virtual circuit and Datagram

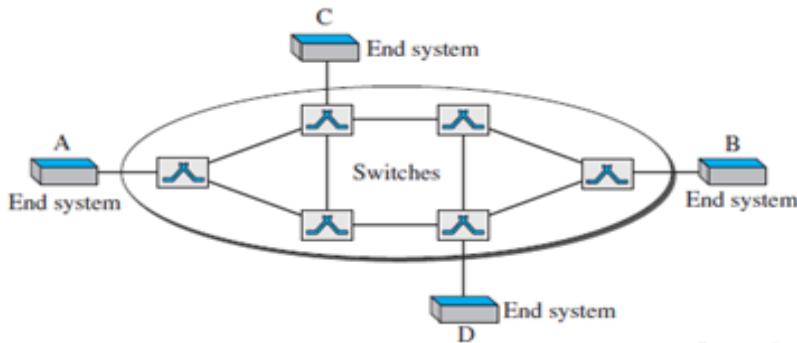
Datagram approach	Virtual circuit approach
In datagram approach, each packet is treated independently, thus they can follow different routes.	In virtual circuit approach, all packets follow the same route.
Packets can arrive at the destination in different order.	Packets should reach the destination in the same order.
Connection establishment is not required before transmission	Connection establishment is required.

**Table 5.3 – Datagram Vs Virtual circuit**

### Virtual-Circuit Networks – characteristics

- A **virtual-circuit network** is a cross between a circuit-switched network and a datagram network. It has some characteristics of both. (Refer fig 5.41).
1. As in a circuit-switched network, there are **setup and teardown phases** in addition to the data **transfer phase**.
  2. Resources can be allocated during the setup phase, as in a circuit-switched network, or on demand, as in a datagram network.
  3. As in a datagram network, data are packetized and each packet carries an address in the header. However, the address in the header has local jurisdiction (it defines what the next switch should be and the channel on which the packet is being carried), not end-to-end jurisdiction. The reader may ask how the intermediate switches know where to send the packet if there is no final destination address carried by a packet. The answer will be clear when we discuss virtual-circuit identifiers in the next section.
  4. As in a circuit-switched network, all packets follow the same path established during the connection.
  5. A virtual-circuit network is normally implemented in the data-link layer, while a Circuit - switched network is implemented in the physical layer and a datagram

network in the network layer. But this may change in the future.



**Fig 5.41 – Virtual circuit network**

### Addressing

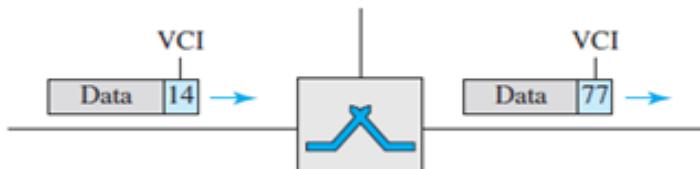
- In a virtual-circuit network, two types of addressing are involved: global and local (virtual-circuit identifier).

#### Global Addressing

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

#### Virtual-Circuit Identifier

- The identifier that is actually used for data transfer is called the **virtual-circuit identifier (VCI)** or the **label**.
- A VCI, unlike a global address, is a small number that has only switch scope; it is used by a frame between two switches. (Refer fig 5.42)



**Fig 5.42 – Virtual circuit identifier**

#### Three Phases

- As in a circuit-switched network, a source and destination need to go through three phases in a virtual-circuit network: **setup, data transfer, and teardown**.
  - In the setup phase, the source and destination use their global addresses to help switches make table entries for the connection.
  - In the teardown phase, the source and destination inform the switches to delete the corresponding entry.
  - Data transfer occurs between these two phases.

**8. Differentiate circuit switching and packet switching with suitable application example (Nov/Dec 2021)**

<b>Circuit switching</b>	<b>Packet switching</b>
In-circuit switching has three phases i) Connection Establishment. ii) Data Transfer. iii) Connection Released	In Packet switching directly data transfer place.
In-circuit switching, each data unit knows the entire path address which is provided by the source.	In Packet switching, each data unit just knows the final destination address intermediate path is decided by the routers.
In-Circuit switching, data is processed at the source system only	In Packet switching, data is processed at all intermediate nodes including the source system.
The delay between data units in circuit switching is uniform.	The delay between data units in packet switching is not uniform.
Resource reservation is the feature of circuit switching because the path is fixed for data transmission.	There is no resource reservation because bandwidth is shared among users.
Circuit switching is more reliable.	Packet switching is less reliable.
Wastage of resources is more in Circuit Switching	Less wastage of resources as compared to Circuit Switching
It is not a store and forward technique.	It is a store and forward technique.
Transmission of the data is done by the source	Transmission of the data is done not only by the source but also by the intermediate routers.
Congestion can occur during the connection establishment phase	Congestion can occur during the data transfer phase
Circuit switching is not convenient for handling bilateral traffic.	Packet switching is suitable for handling bilateral traffic.
Recording of packets is never possible in circuit switching.	Recording of packets is possible in packet switching.
In-Circuit Switching there is a physical path between the source and the destination	In Packet Switching there is no physical path between the source and the destination
Call setup is required in circuit switching	No call setup is required in packet switching.

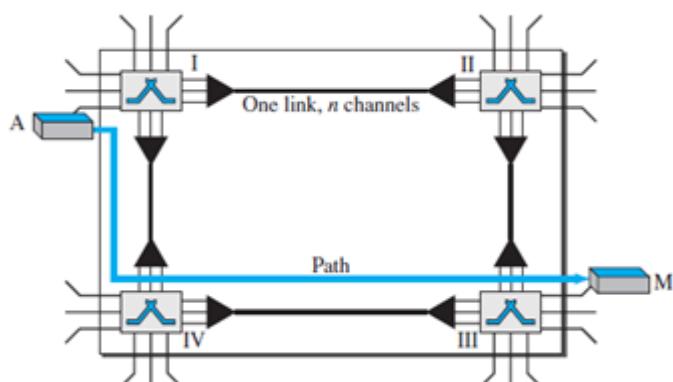
In-circuit switching each packet follows the same route.	In packet switching packets can follow any route.
The circuit switching network is implemented at the physical layer.	Packet switching is implemented at the datalink layer and network layer
Circuit switching requires simple protocols for delivery.	Packet switching requires complex protocols for delivery.

**Table 5.4 circuit switching and packet switching****9. Explain in detail about circuit switched networks****Synopsis:**

- **Introduction**
- **Three Phases**
  - **Setup Phase**
  - **Data-Transfer Phase**
  - **Teardown Phase**

**Introduction:**

- A **circuit-switched network** consists of a set of switches connected by physical links.
- A connection between two stations is a dedicated path made of one or more links.
- However, each connection uses only one dedicated channel on each link.
- Figure 8.3 shows a trivial circuit-switched network with four switches and four links.
- Each link is divided into  $n$  ( $n$  is 3 in the figure) channels by using FDM or TDM (Refer fig 5.43).

**Fig 5.43 – Circuit switched network**

- We have explicitly shown the multiplexing symbols to emphasize the division of the link into channels even though multiplexing can be implicitly included in the switch fabric.
  - The end systems, such as computers or telephones, are directly connected to a switch. We have shown only two end systems for simplicity.
  - When end system A needs to communicate with end system M, system A needs to request a connection to M that must be accepted by all switches as well as by M itself. This is called the **setup phase**; a circuit (channel) is reserved on each link, and the combination of circuits or channels defines the dedicated path. After the dedicated path made of connected circuits (channels) is established, the **data-transfer phase** can take place. After all data have been transferred, the circuits are torn down.
- We need to emphasize several points here:
- ✓ Circuit switching takes place at the physical layer.
  - ✓ Before starting communication, the stations must make a reservation for the resources to be used during the communication. These resources, such as channels (bandwidth in FDM and time slots in TDM), switch buffers, switch processing time, and switch input/output ports, must remain dedicated during the entire duration of data transfer until the **teardown phase**.
  - ✓ Data transferred between the two stations are not packetized (physical layer transfer of the signal). The data are a continuous flow sent by the source station and received by the destination station, although there may be periods of silence.
  - ✓ There is no addressing involved during data transfer. The switches route the data based on their occupied band (FDM) or time slot (TDM). Of course, there is end-to-end addressing used during the setup phase,

### **Three Phases**

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

### **Setup Phase**

- Before the two parties (or multiple parties in a conference call) can communicate, a dedicated circuit (combination of channels in links) needs to be established.
- The end systems are normally connected through dedicated lines to the switches, so connection setup means creating dedicated channels between the switches.
- For example, in Figure 5.44, when system A needs to connect to system M, it sends a setup request that includes the address of system M, to switch I. Switch I finds a channel between itself and switch IV that can be dedicated for this purpose.

- Switch I then sends the request to switch IV, which finds a dedicated channel between itself and switch III. Switch III informs system M of system A's intention at this time.

In the next step to making a connection, an acknowledgment from system M needs to be sent in the opposite direction to system A. Only after system A receives this acknowledgment is the connection established.

#### **Data-Transfer Phase**

- After the establishment of the dedicated circuit (channels), the two parties can transfer data.

#### **Teardown Phase**

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

### **10.Explain in detail about DLC services with framing concepts (HDLC & PPP).**

#### **Synopsis:**

- **Definition**
- **Framing**
- **Byte Oriented protocols**
- **Point-to-Point Protocol (PPP)**
- **Byte-Counting Approach**
- **Bit-Oriented Protocols (HDLC)**
- **Clock-Based Framing (SONET)**
- **Flow and Error Control**
- **Buffers**
- **Error Control**
- **Connectionless and Connection-Oriented**

#### **Definition:**

- The **data link control (DLC)** deals with procedures for communication between two adjacent nodes—node-to-node communication—no matter whether the link is dedicated or broadcast. Data link control functions include *framing* and *flow and error control*.

#### **Framing**

- To transmit frames over the node it is necessary to mention start and end of each frame.
- There are three techniques to solve this frame
  - Byte-Oriented Protocols (BISYNC, PPP, DDCMP)

- Bit-Oriented Protocols (HDLC)
- Clock-Based Framing (SONET)

### **Byte Oriented protocols**

- In this, view each frame as a collection of bytes (characters) rather than a collection of bits.
- Such a byte-oriented approach is exemplified by the BISYNC (Binary Synchronous Communication) see fig.5.44 protocol and the DDCMP (Digital Data Communication Message Protocol).

### **Sentinel Approach**

- The BISYNC protocol illustrates the sentinel approach to framing; its frame format is,

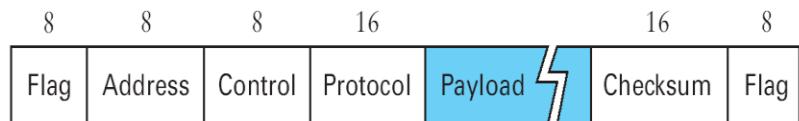


**Fig 5.44 - BISYNC Frame format**

- The beginning of a frame is denoted by sending a special SYN (synchronization) character.
- The data portion of the frame is then contained between special sentinel characters: STX (start of text) and ETX (end of text).
- The SOH (start of header) field serves much the same purpose as the STX field.
- The frame format also includes a field labeled CRC (cyclic redundancy check) that is used to detect transmission errors.
- The problem with the sentinel approach is that the ETX character might appear in the data portion of the frame. BISYNC overcomes this problem by “escaping” the ETX character by preceding it with a DLE (data-link-escape) character whenever it appears in the body of a frame; the DLE character is also escaped (by preceding it with an extra DLE) in the frame body.
- This approach is **called character stuffing**.

### **Point-to-Point Protocol (PPP)**

- The more recent Point-to-Point Protocol (PPP). The format of PPP frame is

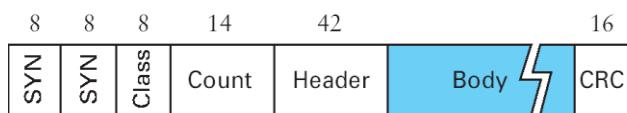


**Fig 5.45 - PPP Frame Format**

- The Flag field has **01111110 as starting sequence.**
- The Address and Control fields usually contain default values
- The Protocol field is used for demultiplexing.
- The frame payload size can be negotiated, but it is 1500 bytes by default.
- The PPP frame format is unusual in that several of the field sizes are negotiated rather than fixed.
- Negotiation is conducted by a protocol called LCP (Link Control Protocol).
- LCP sends control messages encapsulated in PPP frames—such messages are denoted by an LCP identifier in the PPP Protocol.(Refer Fig.5.45)

### Byte-Counting Approach

- The number of bytes contained in a frame can be included as a field in the frame header.
- DDCMP protocol is used for this approach. The frame format is



**Fig 5.46 - DDCMP frame format**

- COUNT Field specifies how many bytes are contained in the frame's body.
- Sometime count field will be corrupted during transmission, so the receiver will accumulate as many bytes as the COUNT field indicates. This is sometimes called a framing error. (Refer Fig.5.46).
- The receiver will then wait until it sees the next SYN character.

### Bit-Oriented Protocols (HDLC)

- In this, frames are viewed as collection of bits. High level data link protocol is used. The format is,



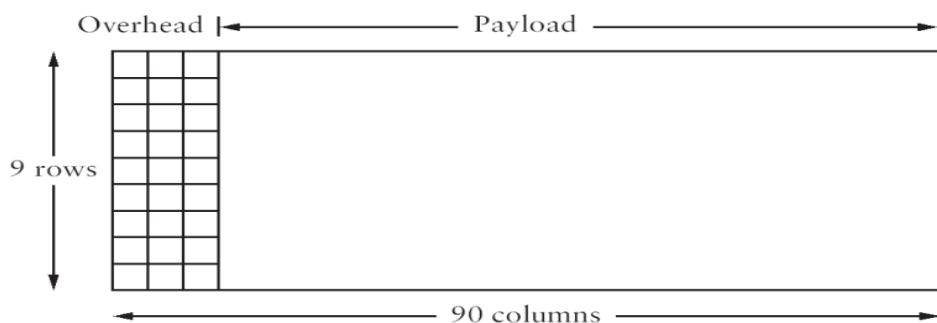
**Fig 5.47 - HDLC Frame Format**

- HDLC denotes both the beginning and the end of a frame with the distinguished bit sequence 01111110.
- This sequence might appear anywhere in the body of the frame, it can be avoided by bit stuffing. (Refer Fig.5.47).

- On the sending side, any time five consecutive 1's have been transmitted from the body of the message (i.e., excluding when the sender is trying to transmit the distinguished 0111110 sequence), the sender inserts a 0 before transmitting the next bit.
  - On the receiving side, five consecutive 1's arrived, the receiver makes its decision based on the next bit it sees (i.e., the bit following the five is).
  - If the next bit is a 0, it must have been stuffed, and so the receiver removes it. If the next bit is a 1, then one of two things is true, either this is the end-of-frame marker or an error has been introduced into the bit stream.
- By looking at the next bit, the receiver can distinguish between these two cases:
1. If it sees a 0 (i.e., the last eight bits it has looked at are 0111110), then it is the end-of-frame marker.
  2. If it sees a 1 (i.e., the last eight bits it has looked at are 0111111), then there must have been an error and the whole frame is discarded.

### Clock-Based Framing (SONET)

- Synchronous Optical Network Standard is used for long distance transmission of data over optical network.
- It supports multiplexing of several low speed links into one high speed links.
- An STS-1 frame is used in this method.



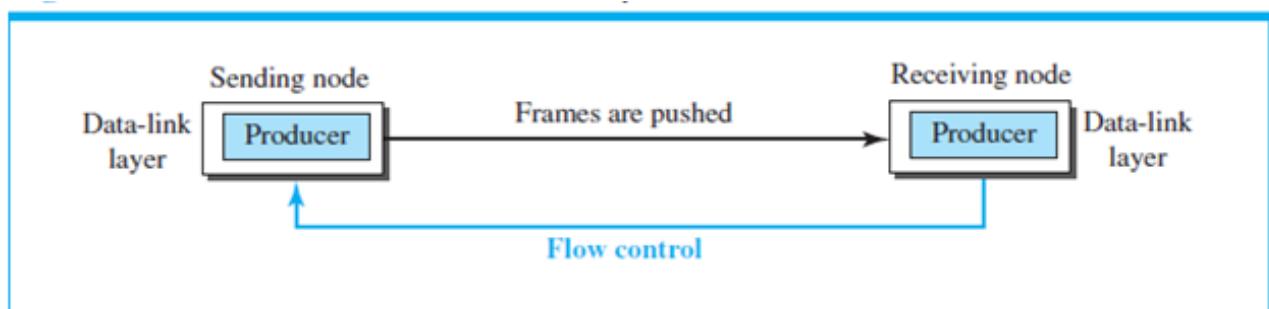
**Fig 5.48 - HDLC Frame Format**

- It is arranged as nine rows of 90 bytes each, and the first 3 bytes of each row are overhead, with the rest being available for data. (Refer Fig.5.48).
- The first 2 bytes of the frame contain a special bit pattern, and it is these bytes that enable the receiver to determine where the frame starts.
- The receiver looks for the special bit pattern consistently, once in every 810 bytes, since each frame is  $9 \times 90 = 810$  bytes long.

### Flow and Error Control

- Whenever an entity produces items and another entity consumes them, there should be a balance between production and consumption rates.

- If the items are produced faster than they can be consumed, the consumer can be overwhelmed and may need to discard some items.
- If the items are produced more slowly than they can be consumed, the consumer must wait, and the system becomes less efficient.
- Flow control is related to the first issue. We need to prevent losing the data items at the consumer site. (Refer fig 5.49)



**Fig 5.49 – Flow control at the data-link layer**

- The figure shows that the data-link layer at the sending node tries to push frames toward the data-link layer at the receiving node.
- If the receiving node cannot process and deliver the packet to its network at the same rate that the frames arrive, it becomes overwhelmed with frames.
- Flow control in this case can be feedback from the receiving node to the sending node to stop or slow down pushing frames.

### Buffers

- Although flow control can be implemented in several ways, one of the solutions is normally to use two *buffers*; one at the sending data-link layer and the other at the receiving data-link 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 the producer.
- When the buffer of the receiving data-link layer is full, it informs the sending data-link layer to stop pushing frames.

### Error Control

- Error control at the data-link layer is normally very simple and implemented using one of the following two methods.
- In both methods, a CRC is added to the frame header by the sender and checked by the receiver.

- ✓ In the first method, if the frame is corrupted, it is silently discarded; if it is not corrupted, the packet is delivered to the network layer. This method is used mostly in wired LANs such as Ethernet.
- ✓ In the second method, if the frame is corrupted, it is silently discarded; if it is not corrupted, an acknowledgment is sent (for the purpose of both flow and error control) to the sender.

### **Connectionless and Connection-Oriented**

- A DLC protocol can be either connectionless or connection-oriented.

#### **Connectionless Protocol**

- In a connectionless protocol, frames are sent from one node to the next without any relationship between the frames; each frame is independent.
- Note that the term *connectionless* here does not mean that there is no physical connection (transmission medium) between the nodes; it means that there is no *connection* between frames. The frames are not numbered and there is no sense of ordering. Most of the data-link protocols for LANs are connectionless protocols.

#### **Connection-Oriented Protocol**

- In a connection-oriented protocol, a logical connection should first be established between the two nodes (setup phase).
- After all frames that are somehow related to each other are transmitted (transfer phase), the logical connection is terminated (teardown phase).
- In this type of communication, the frames are numbered and sent in order. If they are not received in order, the receiver needs to wait until all frames belonging to the same set are received and then deliver them in order to the network layer.
- Connection oriented protocols are rare in wired LANs, but we can see them in some point-to-point protocols, some wireless LANs, and some WANs.