PVP 23

Code: 23EC4602D

III B.Tech - II Semester - Regular Examinations – APRIL 2026

COMPUTER NETWORKS
(ELECTRONICS & COMMUNICATION ENGINEERING)

Duration: 3 hours Max. Marks: 70

Note: 1. This question paper contains two Parts A and B.
2. Part-A contains 10 short answer questions. Each Question carries 2 Marks.
3. Part-B contains 5 essay questions with an internal choice from each unit. Each Question carries 10 marks.
4. All parts of Question paper must be answered in one place.

BL – Blooms Level CO – Course Outcome

PART – A

		BL	CO
1.a)	Name the first four nodes connected in ARPANET.	L1	CO1
1.b)	Compare Bus topology and Mesh topology.	L2	CO1
1.c)	List the types of flow control protocols.	L1	CO2
1.d)	Define Sliding Window Protocol.	L2	CO2
1.e)	Define routing and explain its types.	L1	CO4
1.f)	Give examples of datagram-based protocols.	L2	CO3
1.g)	List the functions of transport layer.	L2	CO3
1.h)	Define flooding in a network.	L1	CO4
1.i)	Give an example of a hierarchical name space used in the Internet.	L1	CO3
1.j)	What is the role of a DNS Resolver?	L1	CO3

PART – B

			BL	CO	Max. Marks
		UNIT-I			
2	a)	Interpret various network topologies in detail.	L2	CO1	5 M
	b)	Discuss about the operation of BISDN with ATM reference model.	L2	CO1	5 M
		OR			
3	a)	Describe the characteristics of LAN and MAN.	L2	CO1	5 M
	b)	Identify the advantages and limitations of wireless transmission media over wired media.	L2	CO1	5 M
		UNIT-II			
4	a)	Compare parity check, CRC and checksum for error detection.	L2	CO2	5 M
	b)	Illustrate the improvements to Stop-and-Wait for better efficiency in long-delay networks.	L3	CO2	5 M
		OR			
5	a)	Demonstrate the role of HDLC in reliable communication over noisy channels.	L3	CO2	5 M
	b)	Solve the 7-bit data 1011010 using even parity.	L3	CO2	5 M

UNIT-III					
6	a)	Compare and contrast a virtual circuit and packet switched network.	L3	CO4	5 M
	b)	Explain the concept of Hierarchical Routing. How does it help in reducing the size of routing tables in large networks?	L2	CO4	5 M
OR					
7	a)	Compare flooding and broadcasting in terms of network efficiency and scalability.	L2	CO4	5 M
	b)	Explain the Bellman-Ford equation? How is it used in distance vector routing?	L2	CO4	5 M
UNIT-IV					
8	a)	Explain about the transmission policy of TCP in the transport layer.	L4	CO3	5 M
	b)	Analyze the congestion control mechanism in transport layer.	L4	CO3	5 M
OR					
9	a)	Draw and explain the TCP segment header and its fields.	L3	CO3	5 M
	b)	Write short notes on performance issues of transport layer.	L3	CO3	5 M
UNIT-V					
10	a)	Summarize the IMAP and MIME with an example.	L2	CO3	5 M
	b)	List and explain five components of multimedia with examples.	L2	CO3	5 M

OR					
11	a)	Describe briefly about World wide web with a neat diagram.	L2	CO3	5 M
	b)	Analyze the architecture of the Electronic mail system with a neat diagram.	L4	CO3	5 M

PVP 23

Code: 23EC4602D

III B.Tech - II Semester - Regular/ Supplementary Examinations APRIL 2026

SUBJECT: COMPUTER NETWORKS

(ELECTRONICS & COMMUNICATION ENGINEERING)

PART - A

1.a) Names of the first four nodes in ARPANET ------- 2M

1.b) Any two comparisons of Bus and Mesh topologies ------- 2M

1.c) Types of flow control protocols. ------- 2M

1.d) Definition of Sliding Window Protocol ------- 2M

1.e) Definition of routing and its types ------- 1+1= 2M

1.f) Any two examples of datagram-based protocols. ------- 2M

1.g) Any two functions of transport layer ------- 2M

1.h) Definition of flooding in a network. ------- 2M

1.i) An example of a hierarchical name space ------- 2M

1.j) The role of a DNS Resolver ------- 2M

PART – B

UNIT – I

2.a) Diagrams + Explanation ------ $2\frac{1}{2}+2\frac{1}{2}=5M$

2.b) Diagrams + Explanation ------ $2\frac{1}{2}+2\frac{1}{2}=5M$

3.a) Diagrams + Explanation ------ $2\frac{1}{2}+2\frac{1}{2}=5M$

3.b) Any five advantages and limitations ------ $2\frac{1}{2}+2\frac{1}{2}=5M$

UNIT - II

4.a) Comparison of parity check, CRC and checksum with examples ---- 5M

4.b) Improvements to Stop-and -Wait protocol ---- 5M

5.a) Frame formats + Explanation ------ **2 + 3 = 5M**

5.b) Solution of the 7-bit data ------ 5M

UNIT – III

6.a) Any five comparisons of virtual circuit and packet switched network ---- 5M

6.b) Routing tables + Explanation ------ $2\frac{1}{2} + 2\frac{1}{2} = 5M$

7.a) Comparison of flooding and broadcasting ------ 5M

7.b) Routing tables + Explanation ------ $2\frac{1}{2} + 2\frac{1}{2} = 5M$

UNIT - IV

8.a) Diagram + Explanation ------ $2 + 3 = 5M$

8.b) Diagram + Explanation ------ $2\frac{1}{2} + 2\frac{1}{2} = 5M$

9.a) Diagram + Explanation ------ $2\frac{1}{2} + 2\frac{1}{2} = 5M$

9.b) Performance issues of transport layer ----- 5M

UNIT – V

10.a) Explanation of **IMAP and MIME** ------ $2\frac{1}{2} + 2\frac{1}{2} = 5M$

10.b) Explanation of Multimedia components ------ 5 M

11.a) Diagram + Explanation ------ $2\frac{1}{2} + 2\frac{1}{2} = 5M$

11.b) Diagram + Explanation ------ $3 + 2 = 5M$

PVP 23

Code: 23EC4602D

III B.Tech - II Semester - Regular/ Supplementary Examinations APRIL 2026

SUBJECT: COMPUTER NETWORKS

(ELECTRONICS & COMMUNICATÍÒN ENGINEERING)

PART - A

1.a) Name the first four nodes connected in ARPANET

1. UCLA 2. UCSB 3. SRI 4. University of Utah

1.b) Compare Bus topology and Mesh topology.

- In **bus topology** all device are connected to a single cable or backbone.
- The cost to implement is low
- In a mesh topology, every device has a dedicated point-to-point link to every other device.
- The cost to implement is higher than other network topologies

1.c) List the types of flow control protocols.

1. Stop-and-Wait Flow Control
2. Sliding Window Flow Control

1.d) Define Sliding Window Protocol.

- This protocol improves the efficiency of stop and wait protocol by allowing multiple frames to be transmitted before receiving an acknowledgment

1.e) Define routing and explain its types.

- **Routing** is the process of selecting a path for data to travel from a source to a destination across a network

Routing algorithms can be grouped into two major classes:

1) Static Routing or Nonadaptive
   - Optimality principle
   - Shortest path algorithm
   - Flooding

2) Dynamic Routing or Adaptive
   - Distance vector routing
   - Link state routing
   - Hierarchical Routing

1.f) Give examples of datagram-based protòcols.

- User Datagram Protocol (UDP)
- Internet Protocol (IP)
- Real-time Transport Protocol (RTP)
- Domain Name System (DNS)

1.g) List the functions of transport layer.

- The network layer provides end-to-end packet delivery using datagrams or virtual circuits.
- Takes data from higher level layers and breaks it into segments that can be sent to lower-level layers for data transmission
- Conversely, reassembles data segments in correct order at destination into data that higher-level protocols and applications can use.
- Uses port addressing

1.h) Define flooding in a network.

- Flooding is **a simple routing technique** in computer networks.In this method Each router forwards the every incoming packet to **all its neighbors** except the line from which it arrived.

1.i) Give an example of a hierarchical name space used in the Internet.

- The hierarchical name space on the Internet is the **Domain Name System (DNS)**.

  Example:
  www.cs.washington.edu

  Breakdown into different domains:

  - .edu → top-level domain (TLD)
  - washington → second-level domain
  - cs → subdomain
  - www → host

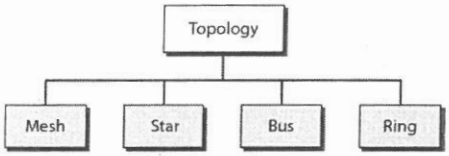
- A domain name is read **from right to left**:

1.j) What is the role of a DNS Resolver?

- A DNS resolver is a specific type of DNS server responsible for translating domain names into internet protocol (IP) addresses.
- When the domain is **remote** and there is **no cached information**, DNS resolution follows a **hierarchical, step-by-step lookup** starting from the root.

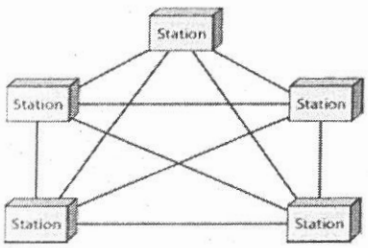
2.a) Interpret various network topologies in detail.

There are four basic topologies possible: mesh, star, bus, and ring

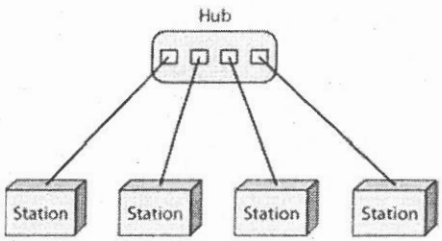


MESH:

- In a mesh topology, every device has a dedicated point-to-point link to every other device. The term *dedicated* means that the link carries traffic only between the two devices it connects.
- A mesh topology can be a **full mesh topology** or a **partially connected mesh topology**
- In a *full mesh topology*, every computer in the network has a connection to each of the other computers in that network.
- To find the number of physical links in a fully connected mesh network with *n* nodes, that each node must be connected to every other node. We need *n(n* - 1) physical links.
- If each physical link allows communication in both directions (duplex mode), The number of connections or duplex-mode links in this network can be calculated using the following formula: **n(n-1) /2**
- In a *partially connected mesh topology*, at least two of the computers in the network have connections to multiple other computers in that network. It is an inexpensive way to implement redundancy in a network.



A fully connected mesh topology



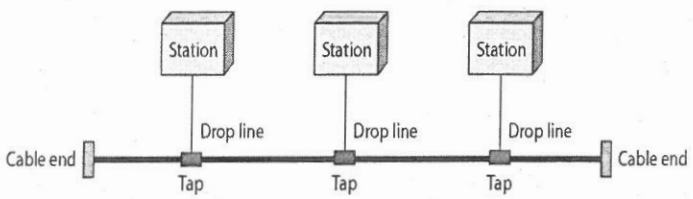
star topology

STAR:

- **A star topology:** In this configuration, every node connects to a central network device, like a hub, switch, or computer. The central network device acts as a server and the peripheral devices act as clients.
- Depending on the type of network card used in each computer of the star topology, a coaxial cable or a RJ-45 network cable is used to connect computers together.

BUS:

- A **line topology or bus topology** is a network setup in which each computer and network device are connected to a single cable or backbone.

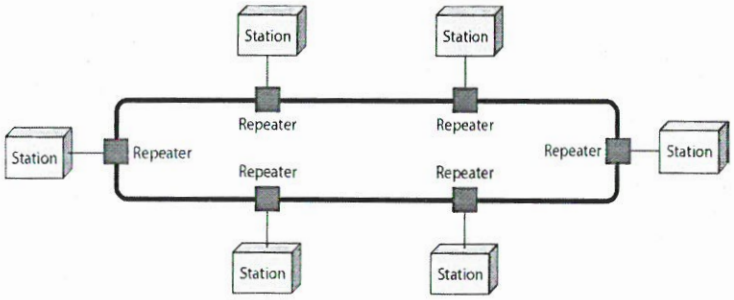


- It's the easiest network topology for connecting computers or peripherals in a linear fashion.
- It requires less cable length than a star topology.
- It can be difficult to identify the problems if the whole network goes down.

RING:

RING: A **ring topology** is a network configuration in which device connections create a circular data path. In a ring network, packets of data travel from one device to the next until they reach their destination.

Most ring topologies allow packets to travel only in one direction, called a **unidirectional** ring network. Others permit data to move in either direction, called **bidirectional**.



- The major disadvantage of a ring topology is that if any individual connection in the ring is broken, the entire network is affected.
- Ring topologies may be used in either local area networks (LANs) or wide area networks (WANs).
- All data flows in one direction, reducing the chance of packet collisions.

2.b) Discuss about the operation of BISDN with ATM reference model.

B-ISDN (Broadband Integrated Services Digital Network)

Broadband ISDN (B-ISDN) is a high-speed network designed to:

- Integrate all types of services (voice, video, data)
- Replace multiple existing networks (telephone, data, cable, etc.)
- Support multimedia applications like:
  - Video on demand
  - High-quality audio
  - High-speed data transfer

- It uses Asynchronous Transfer Mode (ATM) as its core technology.

Asynchronous Transfer Mode (ATM)

- ATM is a cell-switching technology used in B-ISDN.
- The basic idea behind **ATM** is to transmit all information in small, fixed-size packets called cells.
- The cells are 53 bytes long, of which 5 bytes are header and 48 bytes are payload,
- ATM is both a technology (hidden from the users) and potentially a service (visible to the users). Sometimes the service is called **cell relay,** as an analogy to frame relay.

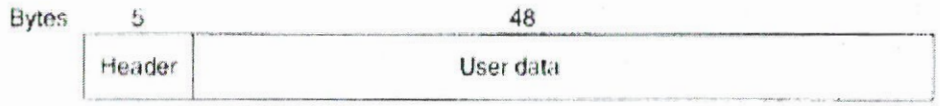


Fig. 1-29. An ATM cell

- ATM networks are connection-oriented. Making a call requires first sending a message to set up the connectio After that, subsequent cells all follow the same path to the destination.
- Cell delivery is not guaranteed, but their order is. If cells 1 and 2 are sent in that order, then if both arrive, they will arrive in that order, never first 2 then **1.**

- ATM networks are organized like traditional WANs, with lines and switches (routers).
- The intended speeds for ATM networks are 155 Mbps and 622 Mbps, with the possibility of gigabit speeds.

The B-ISDN ATM Reference Model

BISDN ATM reference model consists of three layers & 3 Planes:

Three layers: 1. Physical layer 2. ATM. Layer 3. ATM adaptation layer (AAL)
Three planes: 1. User plane 2.Control plane 3. Management plane

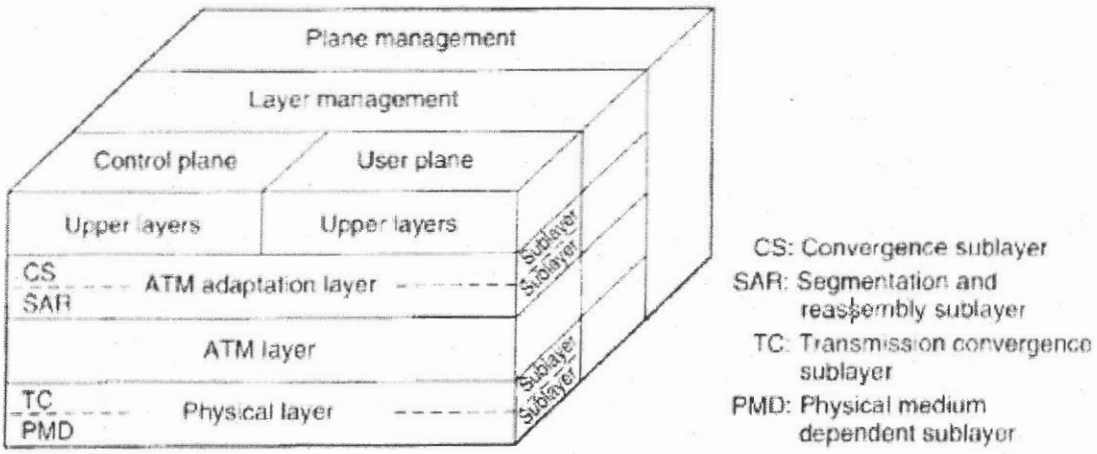


Fig. 1-30. The B-ISDN ATM reference model.

- **The physical layer** deals with the physical medium: voltages, bit timing.
- ATM cells may be sent on a wire or fiber by themselves,
- ATM has been designed to be independent of the transmission medium.
- **The ATM layer** deals with cells and cell transport. It defines the layout of a cell and tells what the header fields mean.
- It also deals with establishment and release of virtual circuits. Congestion control is also located here.

AAL (ATM Adaptation Layer)

- Interface between user applications and ATM

The ATM model is defined as being three-dimensional, as shown in Fig. l-30.

- The **user plane** deals with data transport, flow control, error correction, and other user functions.
- The **control plane** is concerned with connection management.
- The **layer and plane management** functions relate to resource management and interlayer coordination.
- The physical and AAL layers are each divided into two sublayers, one at the bottom that does the work and a convergence sublayer on top that provides the proper interface to the layer above it.
- The PMD (Physical Medium Dependent) sub layer interfaces to the actual cable. It moves the bits on and off and handles the bit timing. For different carriers and cables, this layer will be different.
- The other sublayer of the physical layer is the TC (Transmission Convergence) sublayer.
- When cells are transmitted, the TC layer sends them as a string of bits to the PMD layer. Doing this is easy. At the other end, the TC sublayer gets a pure incoming bit stream from the PMD sublayer.
- The AAL layer is split into a **SAR (Segmentation And Reassembly)** sublayer and a CS **(Convergence Sublayer).**

3.a) Describe the characteristics of LAN and MAN.

Local Area Networks:

- Local area networks, generally called LANs, are privately-owned networks within a single building or campus of up to a few kilometres in size.
- They are widely used to connect personal computers and workstations in company offices and factories to share resources (e.g., printers) and exchange information.
- LANs are distinguished from other kinds of networks by three characteristics:

  (1) Their size,
  (2) Their transmission technology, and
  (3) Their topology.
- LANs are restricted in size. It also simplifies network management
- LANs may use a transmission technology consisting of a cable to which all the machines are attached.
- Traditional LANs run at speeds of 10 Mbps to 100 Mbps, have low delay (microseconds or nanoseconds), and make very few errors. Newer LANs operate at up to 10 Gbps

Various topologies are possible for broadcast LANs.

1. Figure1 shows two of them. In a bus (i.e., a linear cable) network, at any instant at most one machine is the master and is allowed to transmit. All other machines are required to refrain from sending.
2. The arbitration mechanism may be centralized or distributed. IEEE 802.3, popularly called Ethernet. for example, is a bus-based broadcast network with decentralized control, usually operating at 10 Mbps to 10 Gbps.

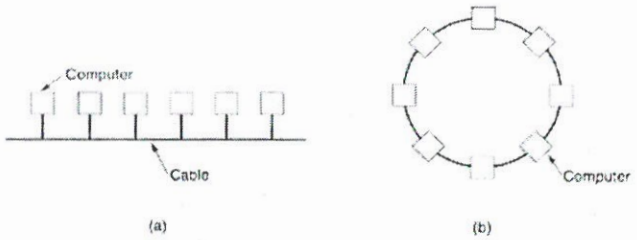


Fig.1.7: Two broadcast networks . (a) Bus. (b) Ring.

- A second type of broadcast system is the ring. In a ring, each bit propagates around on its own, not waiting for the rest of the packet to which it belongs.
- IEEE 802.5 (the IBM token ring), is a ring-based LAN operating at 4 and 16 Mbps. FDDI is another example of a ring network.

Metropolitan Area Network (MAN):

A Metropolitan area network, or MAN, covers a city. The best-known example of a MAN is the cable TV network.

- Design to extend over a large area.
- Connecting number of LAN's to form larger network, so that resources can be shared.
- Networks can be up to 5 to 50 km.
- Owned by organization or individual.
- Data transfer rate is low compare to LAN.

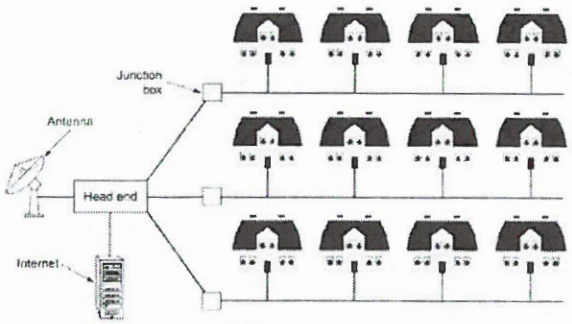


Fig. Metropolitan area network based on cable TV.

- Recent developments in high-speed wireless Internet access resulted in another MAN, which has been standardized as IEEE 802.16 (**wireless MAN**).
- A MAN is implemented by a standard called DQDB (**Distributed Queue Dual Bus**) or IEEE 802.6. DQDB has two unidirectional buses (or cables) to which all the computers are attached.
- Each bus has a head-end, a device that initiates transmission activity. Traffic that is destined for a computer to the right of the sender uses the upper bus. Traffic to the left uses the lower one.

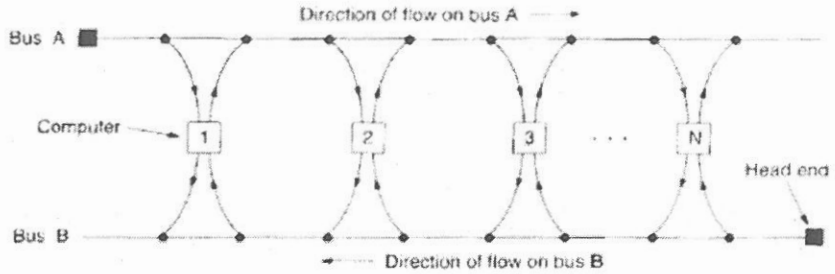


Fig. Architecture of the DQDB metropolitan area network

3.b) Identify the advantages and limitations of wireless transmission media over wired media.

Advantages of Wireless Transmission Media

1. Mobility and Flexibility
   - Users can move freely within coverage area
   - Ideal for mobile devices (phones, laptops, IoT)
2. Easy Installation
   - No need for physical cables
   - Useful in remote, difficult, or temporary locations
3. Cost-Effective (in many cases): Saves cost of laying cables, especially over long distances or rough terrain
4. Scalability: Easy to add new devices without major infrastructure changes
5. Wide Coverage: Can cover large areas using technologies like radio waves, satellites, and cellular networks
6. Supports Modern Applications: Enables Wi-Fi, Bluetooth, mobile communication, and satellite communication

Limitations of Wireless Transmission Media

1. Lower Security
   - Signals travel through air → easier to intercept
   - Requires strong encryption for safety
2. Interference and Noise
   - Affected by:
     - Physical obstacles (walls, buildings)
     - Weather conditions (rain, storms)
     - Other electronic devices
3. Limited Bandwidth: Generally lower data rates compared to wired (like optical fiber)
4. Reliability Issues
   - Signal strength may fluctuate
   - Connection drops may occur
5. Higher Error Rate : More prone to noise → higher chances of data errors
6. Range Limitations
   - Coverage area is limited (except satellites)
   - Needs repeaters or base stations

UNIT-2

4.a) Compare parity check, CRC and checksum for error detection.

Three different error-detecting codes. They are all linear, systematic block codes:

1. Parity.
2. Checksums.
3. Cyclic Redundancy Checks (CRCs)

1. In **Parity Check** a single parity bit is appended to the data. The parity bit is chosen so that the number of 1 bits in the codeword is even (or odd). Doing this is equivalent to computing the (even) parity bit as the modulo 2 sum or XOR of the data bits.

- it can detect single-bit errors.

For example, when 1011010 is sent in even parity, a bit is added to the end to make it 10110100. With odd parity 1011010 becomes 10110101.

2.Checksum

- In checksum error detection scheme, the data is divided into fixed size k segments each of m bits.
- In the sender's end the segments are added using 1's complement arithmetic to get the sum. The sum is complemented to get the checksum.
- The checksum segment is sent along with the data segments.
- At the receiver's end, all received segments are added using 1's complement arithmetic to get the sum. The sum is complemented.
- If the result is zero, the received data is accepted; otherwise discarded.

Original Data

10011001	11100010	00100100	10000100
1	2	3	

k=4, m=8

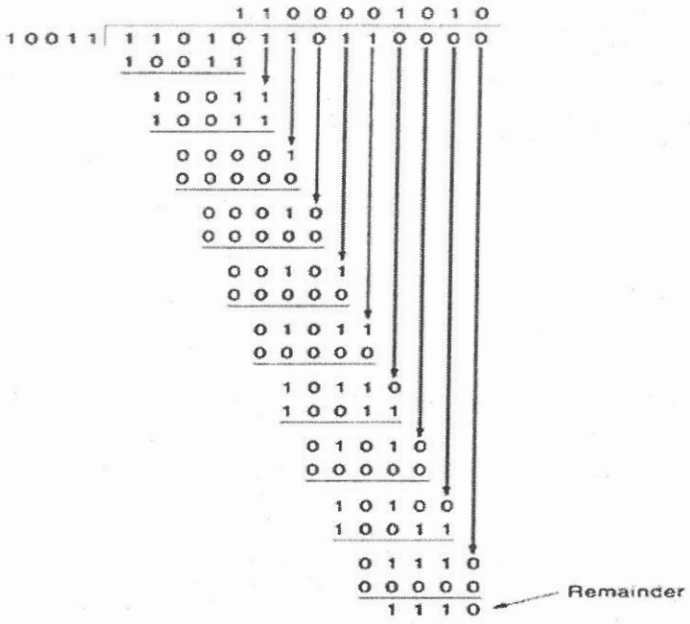
Sender

```
1        10011001
2        11100010
        ---------
       (1)01111011
                1
        ---------
         01111100
3        00100100
        ---------
         10100000
4        10000100
        ---------
       (1)00100100
                1
        ---------
Sum:     00100101
        ---------
CheckSum: 11011010
```

3. Cyclic redundancy check (CRC) or Polynomial code

- In CRC, a sequence of redundant bits, called cyclic redundancy check bits, are appended to the end of data unit so that the resulting data unit becomes exactly divisible by binary number.
- At the destination, the incoming data unit is divided by the same number. If at this step there is no remainder, the data unit is assumed to be correct and is therefore accepted.
- A remainder indicates that the data unit has been damaged in transit and therefore must be rejected.
- To compute the checksum for some frame with m bits, corresponding to the polynomial M(x), the frame must be longer than the generator polynomial.

Frame : 1 1 0 1 0 1 1 0 1 1
Generator: 1 0 0 1 1
Message after 4 zero bits are appended: 1 1 0 1 0 1 1 0 1 1 0 0 0 0



Transmitted frame: 1 1 0 1 0 1 1 0 1 1 1 1 0

4.b) Illustrate the improvements to Stop-and -Wait for better efficiency in long delay networks.

- The most unrealistic restriction used in protocol 1: the ability of the receiving network layer to process incoming data infinitely quickly
- The main problem we have to deal with here is how to prevent the sender from flooding the receiver.
- If the network designers can calculate the worst-case behaviour of the receiver, they can program the sender to transmit so slowly that even if every frame suffers the maximum delay, there will be no overruns.
- The trouble with this approach is that it is too conservative. It leads to a bandwidth utilization that is far below the optimum, unless the best and worst cases are almost the same

The Improvement: Feedback-Based Flow Control

- A more general solution to this dilemma is to have the receiver provide feedback to the sender.
- The receiver explicitly tells the sender when to send the next frame.

Mechanism:

- Sender sends **1 frame**
- Receiver processes it
- Receiver sends **ACK (permission signal)**
- Sender sends next frame **only after ACK**

- This is the **Stop-and-Wait protocol**. This prevents **receiver overflow** and ensures safe communication.

A Simplex Protocol for a Noisy Channel

- Now let us consider the normal situation of a communication channel that makes errors. Frames may be either damaged or lost completely.

- However, we assume that if a frame is damaged in transit, the receiver hardware will detect this when it computes the checksum. If the frame is damaged in such a way that the checksum is nevertheless correct.

Sender retransmits if ACK not received (using timer)

- Sender sends Frame 1, Receiver gets it
- Receiver sends ACK, if ACK is lost, Sender times out then retransmits Frame 1
- Receiver **accepts duplicate frame**
- Duplicate data delivered → **data corruption**

The **Improvement:** Add a **sequence number** to each frame

- When a frame containing the correct sequence number arrives, it is accepted and passed to the network layer.
- Any arriving frame containing the wrong sequence number is rejected as a duplicate.

Improvement in Protocol: Stop-and-Wait ARQ (PAR)

- Stop-and-Wait evolves from a **flow-control mechanism** into a **reliable communication protocol** by adding:
  - ACKs
  - Timers
  - Sequence numbers
- Protocols in which the sender waits for a positive acknowledgement before advancing to the next data item are often called PAR (Positive Acknowledgement with Retransmission) or ARQ (Automatic Repeat reQuest).
- This protocol transmits data only in one direction.

Improvement: Full-Duplex Communication

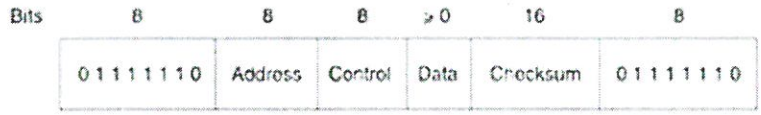
- Both sides send data simultaneously.
- ACKs can be embedded in reverse traffic → reduces idle time.

5.a) Demonstrate the role of HDLC in reliable communication over noisy channels.

HDLC—High-Level Data Link Control

HDLC, is a classical bit-oriented data link layer protocol and uses bit stuffing for data transparency

- HDLC derived from the data link protocol first used in the IBM mainframe world: SDLC (Synchronous Data Link Control) protocol.
- All the bit-oriented protocols use the frame structure shown in Fig. 3-24.
- The Address field is primarily of importance on lines with multiple terminals, where it is used to identify one of the terminals. For point-to-point lines, it is sometimes used to distinguish commands from responses.

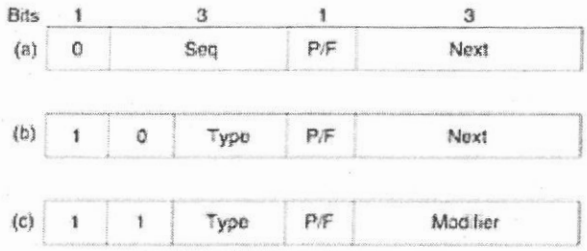


Frame format for bit-oriented protocols.

Flag: 01111110 → Marks beginning and end

- The Address field: Identifies station with in multiple terminals.
- The Control field is used for sequence numbers, acknowledgements, and other purposes.
- The Data field may contain any information.
- The Checksum field is a cyclic redundancy code for error detection

Figure 3-25. Control field of (a) an information frame, (b) a supervisory frame, (c) an unnumbered frame.



- The P/F bit stands for Poll/Final. It is used when a computer (or concentrator) is polling a group of terminals.

Information Frame (I-frame)

- Carries user data
- Contains:
  - Sequence number (Seq)
  - Acknowledgement (Next)
- Used for data transmission

Supervisory frames:

- The various kinds of Supervisory frames are distinguished by the Type field.
- Type 0 is an acknowledgement frame (officially called RECEIVE READY) used to indicate the next frame expected. This frame is used when there is no reverse traffic to use for piggybacking.
- Type 1 is a negative acknowledgement frame (officially called REJECT). It is used to indicate that a transmission error has been detected
- Type 2 is RECEIVE NOT READY. It acknowledges all frames up to but not including Next, just as RECEIVE READY does, but it tells the sender to stop sending.

Unnumbered frame. It is sometimes used for control purposes but can also carry data when unreliable connectionless service is called for.

5.b) Solve the 7-bit data 1011010 using even parity.

Given data: **1011010**

Check parity condition

- Even parity requires the **total number of 1s to be even**
- Current count = **4 (already even)**

  Since 4 is already **even, no need to add a 1**

  So, the **parity bit = 0**

Final codeword

with parity bit added at the end : **10110100**

If the parity bit is added at the beginning: **01011010**

6.a) Compare and contrast a virtual circuit and packet switched network.

Issue	Packet Switched Network	Virtual-circuit subnet
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC

Virtual-Circuit Network Operation

In a virtual-circuit network, communication follows these steps:

- Setup Phase – A virtual circuit is established by sending a setup request through the network
- Data Transfer – All packets follow the predetermined path using the assigned VC number
- Teardown Phase – The virtual circuit is released when communication ends

- The issue with virtual circuits is that each time a new connection is set up, resources and extra information have to be reserved at every router along the path,
- It is used by the ATM networks, traditional telephone systems

Datagram Network Operation

In packet switched networks, each packet is treated independently:

- **Individual Routing** – Each packet contains complete addressing information
- **Dynamic Path Selection** – Routers make forwarding decisions based on current network conditions
- **No State Information** – Network devices don't maintain connection state

- The major drawback of packet switched network is no delivery guarantee of packets.
- It is used by the Internet Protocol (IP), UDP-based communications

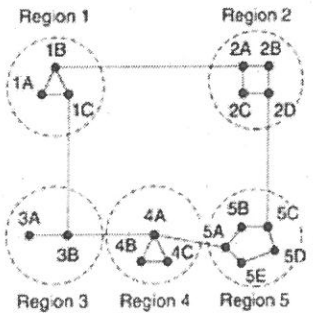
6.b) Explain the concept of Hierarchical Routing. How does it help in reducing the size of routing tables in large networks?

- Hierarchical routing is a technique used to **reduce the size of routing tables** in large networks by organizing routers into groups (called *regions* or *levels*) instead of having every router know everything about the entire network.
- The Problems in Large Networks are:

1. the router routing tables grow proportionally
2. memory consumed by ever-increasing tables,
3. more CPU time is needed to scan them
4. more bandwidth is needed to send status reports about them.

To overcome the above problems hierarchical routing is used

- When hierarchical routing is used, the routers are divided into groups called as regions, with each router knowing all the details about how to route packets to destinations within its own region, but knowing nothing about the internal structure of other regions.
- For huge networks, a two-level hierarchy may be insufficient; it may be necessary to group the regions into clusters, the clusters into zones, the zones into groups, and so on, until we run out of names for aggregations.
  - Figure 5-15 gives a quantitative example of routing in a two-level hierarchy with five regions. The full routing table for router 1A has 17 entries, as shown in Fig. 5-15(b).
  - When routing is done hierarchically, as in Fig. 5-15(c), there are entries for all the local routers as before, but all other regions have been condensed into a single router, so all traffic for region 2 goes via the 1B -2A line, but the rest of the remote traffic goes via the 1C -3B line.
  - Hierarchical routing has reduced the table from 17 to 7 entries. As the ratio of the number of regions to the number of routers per region grows, the savings in table space increase.



(a)

Full table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

(b)

Hierarchical table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

(c)

Figure 5-15. Hierarchical routing

- For example, the best route from 1A to 5C is via region 2, but with hierarchical routing all traffic to region 5 goes via region 3, because that is better for most destinations in region 5.
- Kamoun and Kleinrock (1979) discovered that the optimal number of levels for an N router subnet is ln N, requiring a total of e ln N entries per router.
- They have also shown that the increase in effective mean path length caused by hierarchical routing is sufficiently small that it is usually acceptable.

7.a) Compare flooding and broadcasting in terms of network efficiency and scalability.

Flooding is a routing technique in which each incoming packet is forwarded on all outgoing links except the line it arrived on.

Network Efficiency of Flooding is **very low** efficiency

The major disadvantage of this algorithm is that

- it generates too many duplicate packets
- consumes too much bandwidth
- causes **congestion**
- Extra overhead due to:
  - Maintaining sequence number lists
  - Processing duplicate packets

- Flooding is controlled using:
  - Hop count (limits lifetime)
  - Sequence numbers (avoid duplicates)
  - Selective flooding (send only in likely direction)

- Scalability of Flooding is **poor**.
  - Traffic grows exponentially with network size
  - Routers must store sequence number tables
  - Not suitable for large networks

Broadcast Routing

- Broadcasting means sending a packet from one source to all destinations (nodes) in the network simultaneously.

- Uses **controlled methods**, such as:
- Multicasting
- Spanning tree
- Reverse path forwarding

- **Network Efficiency of Broadcasting is much higher than flooding**
  - Avoids unnecessary duplicates
  - Uses **optimized paths**
  - Reduces bandwidth usage

- **Scalability of Broadcasting is good.**
  - Traffic grows **linearly or moderately**, not exponentially
  - Suitable for **large networks**

7.b) Explain the Bellman-Ford equation? How is it used in distance vector routing?

Distance Vector Routing

- Modern computer networks generally use dynamic routing algorithms rather than the static ones because static algorithms do not take the current network load into account.
- Distance vector is the "Dynamic Routing" algorithm. Distance vector routing algorithm also called as **Bellman-Ford algorithm** or Ford Fulkerson algorithm used to calculate the shortest path.
- It was the original ARPANET routing algorithm and was also used in the Internet under the name RIP.
- Distance vector routing algorithms operate by having each router maintain a table (i.e, a vector) giving the best known distance to each destination.
- These tables are updated by exchanging the information with the neighbor having a direct link. Tables contain one entry for each router, this entry contains two parts: the preferred outgoing line used to reach the destination or an estimate of the time or distance to that destination.
- The metric used can be the number of hops required to reach from source to destination. Time delay in milliseconds, total number of packets queued along the path.
- As an example, assume that delay is used as a metric and that the router knows the delay to each of its neighbors. Once every T msec each router sends to each neighbour a list of its estimated delays to each destination.
- The Each router sends its distance vector (its table of best-known distances to all destinations) to its neighbors. It also receives distance vectors from neighbors.

Example: If neighbor X says estimate delay to router i is X_i

The delay from current router to X is m msec

Then delay (Distance) to router i via X = $(X_i + m)$ msec

- The router computes the delay for all neighbors and find out which estimate seems the best (minimum) and use that estimate and the corresponding line in its new routing table.

This updating process is illustrated in Fig. 5-9. Part (a) shows a subnet. The first four columns of part (b) show the delay vectors received from the neighbors of router J.

- A claims to have a 12-msec delay to B, 25-msec delay to C, a 40-msec delay to D, etc.
- Suppose that J has measured or estimated its delay to its neighbors, A, I, H, and K as 8, 10, 12, and 6 msec respectively.
  i.e Router J has neighbors: A (8ms away), I (10ms away), H (12ms away), K (6ms away)

The neighbors A, I, H, and K reports its distance to Router G: A (18ms away) , I (31ms away), H (6ms away), K (31ms away)

Now J computes its new route to router G:
J computes the delay to *G* via A, *I*, *H*, and *K*

delay via A: 18 + 8 = 26 ms
delay via I : 31 + 10 = 41 ms
delay via H : 6 + 12 = 18 ms
delay via K : 31 + 6 = 37 ms

The best of these values is 18, so it makes an entry in its routing table that the delay to G is 18msec and that the route to use is via H. So router J updates its routing table:

Destination: G Cost: 18 ms Next hop: H

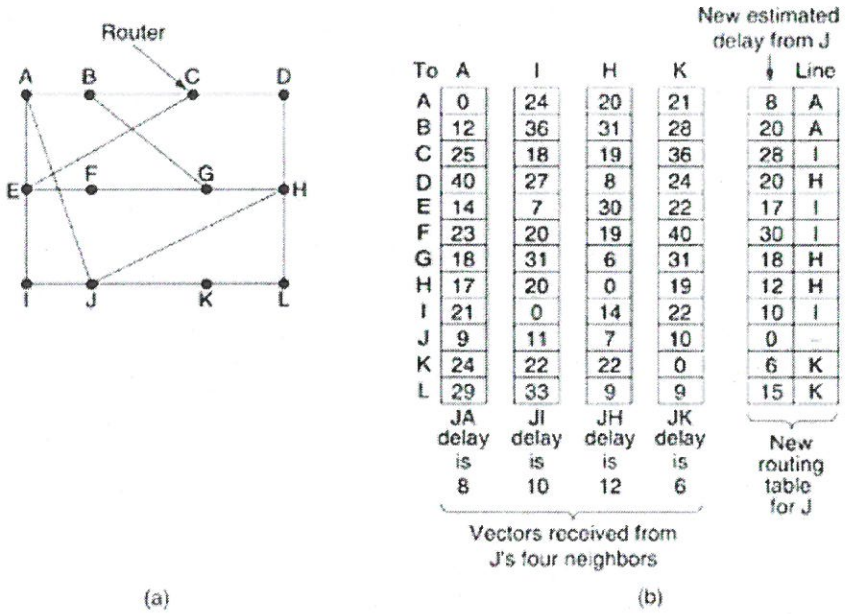


Fig. 5-9.(a) A subnet. (b) Input from **A, I, H, K,** *and the new routing table for* **J.**

UNIT-4

8.a) Explain about the transmission policy of TCP in the transport layer.

TCP transmission policy refers to the **rules TCP follows to decide *when and how much data to send*** into the network. It controls the flow of segments from sender to receiver to ensure efficiency and avoid congestion.

TCP Window Management:

- Window management in TCP is not directly tied to acknowledgements as it is in most data link protocols.
- **In TCP, window size and acknowledgements are independent.**
  ACK → tells what data is received
  Window → tells how much more data can be sent

For example, suppose

- the receiver has a 4096-byte buffer (memory), as shown in Fig. 6-34 .
- If the sender transmits a 2048-byte segment with SEQ = 0, that is correctly received,
- the receiver will acknowledge the segment (ACK = 2048, WIN = 2048) i.e the receiver now has only 2048 bytes of buffer space free and the sender can send 2048 more bytes of data.
- Now the sender transmits another 2048 bytes, with SEQ = 2048

  Receiver replies: Buffer becomes full ACK = 4096, WIN = 0 (advertised window is 0.)

  When WIN = 0: Sender must stop sending
- When the window is 0, the sender may not normally send segments, but with two exceptions:
  1. urgent data may be sent (example, to allow the user to kill the process running on the remote machine)
  2. the sender may send a 1-byte segment to make the receiver reannounce the next byte expected and window size.
- TCP does NOT require: Immediate sending of data & Immediate ACKs.

Example:

Instead of sending 2 KB twice, TCP could wait and send **4 KB at once.** This freedom can improve performance.

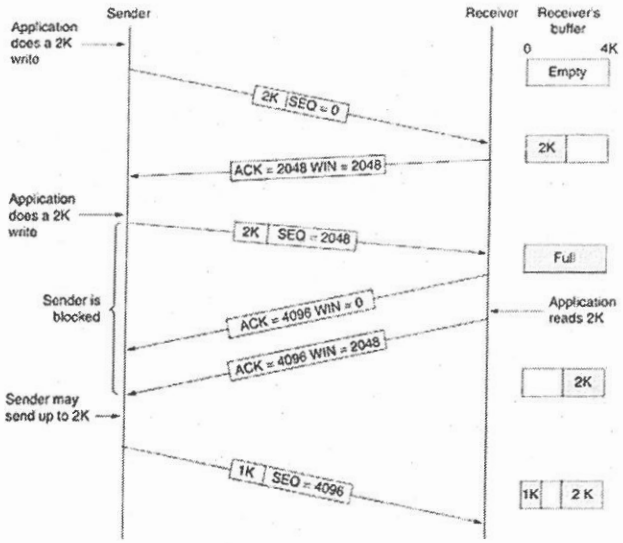
Problem: Inefficient Small Packets

Example: typing in **Telnet for 1 character**: 41-byte data packet sent

- 40-byte ACK
- 40-byte window update
- 41-byte echo

- In all, total **162 bytes** of bandwidth are used and four segments are sent for each character typed.
- One approach that many TCP implementations use to optimize this situation is to delay acknowledgements and window updates for 500 msec.

Figure 6-34. Window management in TCP.



8.b) Analyze the congestion control mechanism in transport layer.

- TCP tries to **avoid congestion** before it occurs.

Hydraulic Analogy

- In Fig. 6-36, this problem illustrated hydraulically.
  - **Receiver limit** = bucket size
  - **Network limit** = pipe/funnel capacity

Fast network → slow receiver (Fig. 6-36(a))

- The **pipe is wide** → network can carry data easily
- The **bucket is small** → receiver has limited buffer

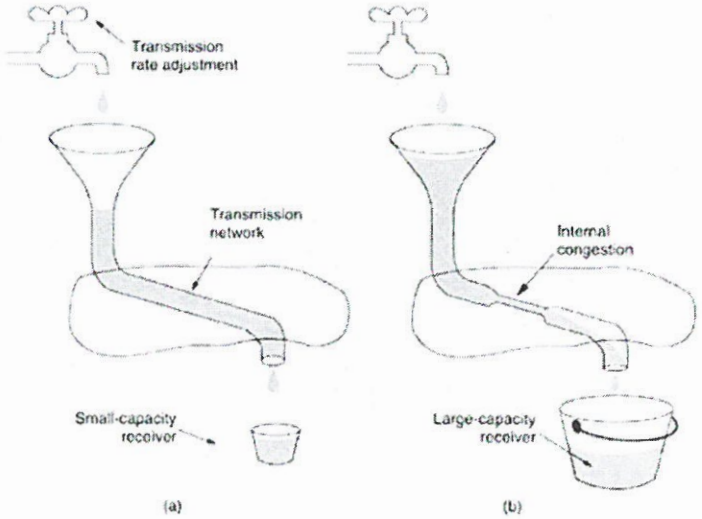
- In Fig. 6-36(a), a thick pipe leading to a small-capacity receiver. As long as the sender does not send more water than the bucket can contain, no water will be lost.

Slow network → fast receiver Fig. 6-36(b)

- The **pipe is narrow/curved** → limited network capacity
- The **bucket is large** → receiver can handle lots of data

- In Fig. 6-36(b) the limiting factor is not the bucket capacity, but the internal carrying capacity of the network. If too much water comes in too fast, it will back up and some will be lost (in this case by overflowing the funnel).

Figure 6-36. (a) A fast network feeding a low-capacity receiver. (b) A slow network feeding a high-capacity receiver.



When data is sent over a network, TCP must handle two potential problems:

1. **Receiver Capacity (Flow Control)** → how much data the receiver can handle (buffer size).
2. **Network Capacity (Congestion control)** → how much data the network can carry without congestion.

- In **hydraulic analogy** TCP solves those problems by maintaining two separate windows:
  - **Receiver Window (rwnd)** → set by the receiver to avoid receiver overflow
  - **Congestion Window (cwnd)** → set by the sender based on network conditions to avoid network congestion
- Each window reflects the number of bytes the sender may transmit. The number of bytes that may be sent is the minimum of the two windows.

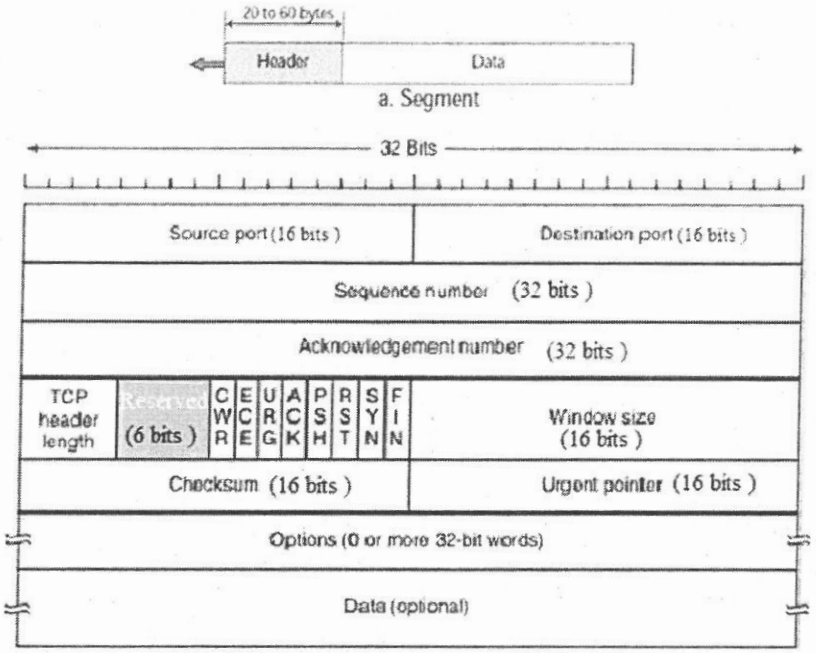
  The actual amount of data sent is: **Effective Window = min(rwnd, cwnd)**
- TCP avoids congestion by **respecting the minimum of receiver capacity and network capacity**, using rwnd and cwnd together.
- If receiver allows 8 KB but network can handle only 4 KB → send **4 KB**
- If receiver allows 8 KB and network can handle up to 32 KB → send **8 KB**

Slow start algorithm:

- When a connection is established, the sender initializes the congestion window to the size of the maximum segment in use on the connection. It then sends one maximum segment.
- If this segment is acknowledged before the timer goes off, it adds one segment's worth of bytes to the congestion window to make it two maximum size segments and sends two segments.
- As each of these segments is acknowledged, the congestion window is increased by one maximum segment size.
- Slow start continues until a timeout occurs or the receiver's window limit is reached.

9.a) Draw and explain the TCP segment header and its fields.

- Every TCP segment consists of a 20 byte fixed format header. Header options may follow the fixed header. With a header so that it can tag up to 65535 data bytes.



TCP Segment Header

Source Port: 16 Bit number which identifies the Source Port number (Sending Computer's TCP Port).

Destination Port: 16 Bit number which identifies the Destination Port number (Receiving Port).

Sequence Number: The sequence number of the first data byte in this segment.

Acknowledgement Number: If the ACK control bit is set, this 32 Bit number field which indicates the next sequence number that the receiving device is expecting to receive.

Header Length : 4 Bit field which shows the number of 32 Bit words in the header.

Reserved (6 bit): It is reserved for future use and always set to 0 (Size 6 bits).

Control flags – TCP uses 8 control flags to manage data flow in specific situations.

1. **ECE :** Explicit **Congestion Notification** Echo (ECN-Echo)
2. **CWR** (Congestion Window Reduced) → **Response to congestion**

- **URG:** Urgent pointer field is used to indicate a byte offset from the current sequence number at which urgent data are to be found.

3. **ACK:** Acknowledgement number field

- The ACK bit is set to 1 to indicate that the Acknowledgement number is valid. If ACK is 0, the segment does not contain an acknowledgement, so the Acknowledgement number field is ignored.

4. **PUSH:** The PUSH flag is set or reset according to a data type that is sent immediately or not.
5. **RST:** It Resets the connection.
6. **SYN:** The SYN bit is used to establish connections and synchronizes the sequence number.
7. **FIN:** The FIN bit is used to release a connection. It specifies that the sender has no more data to transmit.

Window: It is used in Acknowledgement segment. Indicates the size of the receive window,

Checksum field is used to checksum the header, data, and a conceptual pseudoheader for error-checking.

Urgent Pointer: Shows the end of the urgent data so that interrupted data streams can continue. When the URG bit is set, the data is given priority over other data streams (Size 16 bits).

Options: The Options field provides a way to add extra facilities not covered by the regular header.

Data: Although in some cases like acknowledgement segments with no data in the reverse direction, the variable-length field carries the application data from sender to receiver.

9.b) Write short notes on performance issues of transport layer.

1. Congestion and Window Size Problems
   - With TCP, performance heavily depends on the congestion window and flow control window.
   - If the sender's window is too small, it limits throughput. If the network is congested, TCP reduces its sending rate.

2. Packet Loss & Retransmissions
   - TCP guarantees delivery, so when packets are lost, they're retransmitted. It causes network congestion and reduces speed

3. Flow Control (Receiver Window Limits)
   - TCP uses a sliding window to control how much data can be sent before receiving ACKs.
   - If the receiver processes data slowly, the sender is forced to wait and it results underutilization of available bandwidth

4. Latency and Round-Trip Time (RTT)
   - TCP requires acknowledgments (ACKs), so performance depends on RTT.
   - If RTT is high, slower data transfer (especially noticeable in long-distance connections) and slower page loads, delayed responses

5. Connection Setup Overhead
   - TCP requires a three-way handshake before data transfer.
   - The problem with this TCP connection establishment is it adds delay, especially for short-lived connections.

10.a) Summarize the IMAP and MIME with an example.

IMAP - The Internet Message Access Protocol

- IMAP is an **email access protocol** used for retrieving and managing emails **directly on the mail serv**
- IMAP Version 4 of the protocol is defined in RFC 3501.
- To use IMAP, the mail server runs an IMAP server that listens to port 143.
- The user agent runs an IMAP client. The client connects to the server and begins to issue commands

Key Features

- Folder (Mailbox) Management
  - Users can organize emails into folders (Inbox, Sent, etc.)
- Access from Multiple Devices
  - Emails remain on server → accessible anywhere
- Search on Server
  - Find emails using criteria (e.g., sender, subject)
- Selective Fetching
  - Download full message or only parts (e.g., headers)
- Message Flags
  - Mark emails as read, unread, deleted, etc.

Common Commands (Examples)

- LOGIN → Authenticate user
- SELECT → Open a folder
- FETCH → Retrieve messages
- SEARCH → Find specific emails
- STORE → Change message status
- EXPUNGE → Delete marked emails

➢ IMAP is an improvement over an earlier final delivery protocol, POP3 (Post Office Protocol, version 3 which is specified in RFC 1939. POP3 is a simpler protocol but supports fewer features and is less secu in typical usage. Downloads emails to one device

Example

- Check your email on mobile and laptop:
  - You delete a message on mobile
  - It disappears on laptop too

➢ This happens because IMAP synchronizes emails on the server

MIME (Multipurpose Internet Mail Extensions). It is widely used for mail messages that are sent across the Internet.

MIME defines five new message headers, as shown in Fig. 7-12. The first of these simply tells the user agent receiving the message that it is dealing with a MIME message, and which version of MIME it uses. Any messa not containing a MIME-Version: header is assumed to be an English plaintext message (or at least one using only ASCII characters) and is processed as such.

Header	Meaning
MIME-Version:	Identifies the MIME version
Content-Description:	Human-readable string telling what is in the message
Content-Id:	Unique identifier
Content-Transfer-Encoding:	How the body is wrapped for transmission
Content-Type:	Type and format of the content

Figure 7-12. Message headers added by MIME.

Key Features

- Supports **multiple content types**
- Uses **encoding schemes** (e.g., Base64) for binary data
- Allows **multipart messages**

Example

➢ Sending an email with:
  - A **PDF attachment**
  - An **image file**

➢ MIME encodes these files so they can be transmitted via email systems.

10.b) List and explain five components of multimedia with examples.

- Multimedia, they generally mean the combination of two or more continuous media. In practice, the t media are normally audio and video, that is, sound plus moving pictures.
- The five core components of multimedia are text, images, audio, video, and animation

1. **Text (Text):**

- The basic element of multimedia used to display titles, menus, and written information. It is crucial for providing precise information to the audience.
  Examples: Documents, subtitles, headlines in a digital article, or text within a graphical interface.

2. **Graphics/Images (Graphics)**

- Still pictures, photographs, diagrams, or illustrations that support the text and make the content more engaging.
  Examples: JPEG photographs, PNG icons, infographics, and illustrations.

3. **Audio (Audio)**

- Any sound produced, including speech, music, or sound effects, which adds an auditory dimension to the multimedia experience.
  Examples: Voice-over narration, background music, sound effects in a video, or audio narration in an interactive app.

4. **Video (Video)**

- The recording and display of moving images, often combined with sound, offering a powerful, dynamic way to convey information.
  Examples: Live action recordings, movie clips, YouTube videos, or streaming content.

5. **Animation (Animation)**

- A sequence of still images played in rapid succession to create the illusion of movement, often used to simulate real-world actions or make interfaces more attractive.
  Examples: 2D animated characters, 3D animated infographics, GIF images, or moving transitions on a website

11.a) Describe briefly about World Wide Web with a neat diagram.

- The World Wide Web is an architectural framework for accessing linked documents spread out over millions of machines all over the Internet.
- Web is a **huge collection of documents (called Web pages)** available all over the world. These pages are connected to each other.
- The idea of having one page point to another is called **hypertext**.
- Each Web page can contain **links to other pages**. These links are called **hyperlinks**.
- When you **click a hyperlink**, you are taken to another page.
- The browser is displaying a Web page on the client machine. This page may contain **hyperlinks**.
- When the user clicks on a line of text that is linked to a page on the abcd.com server, the browser follows the hyperlink by sending a request message to the abcd.com server asking it for the page.

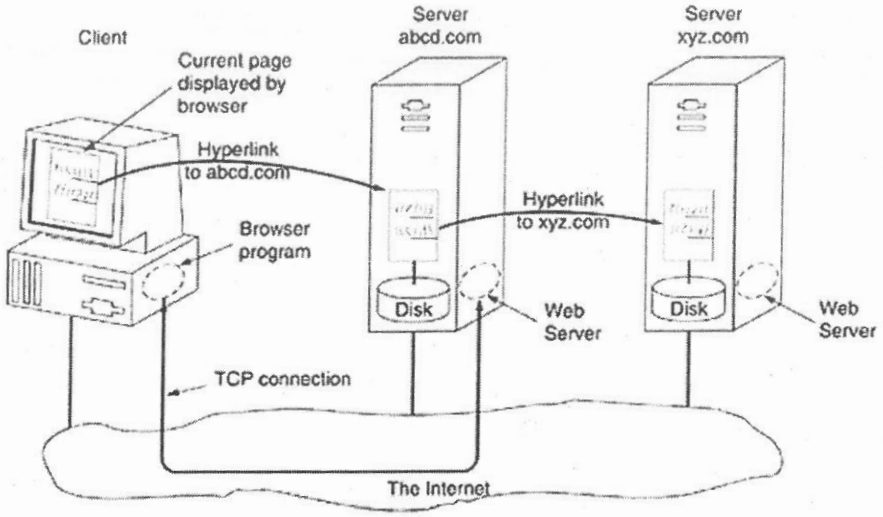


Figure 7-19. The parts of the Web model

- When the page arrives, it is displayed. If this page contains a hyperlink to a page on the xyz.com server that is clicked on, the browser then sends another request to to the xyz.com server.
- That server responds with its page.
- The browser displays it
  - Clicking a hyperlink makes the browser **contact another server**
  - The server **sends the requested page**
  - The browser **displays it**
  - This process can continue endlessly across different websites

11.b) Analyze the architecture of the Electronic mail system with a neat diagram.

- **Electronic mail** (**email** or **e-mail**) is a method of exchanging digital messages ("mail") between people using electronic devices.
- Email is one of the protocols included with the Transport Control Protocol/Internet Protocol (TCP/IP) suite of protocols.
- A popular protocol for sending email is Simple Mail Transfer Protocol (SMTP), and a popular protocol for receiving it is Post Office Protocol 3 (POP3).

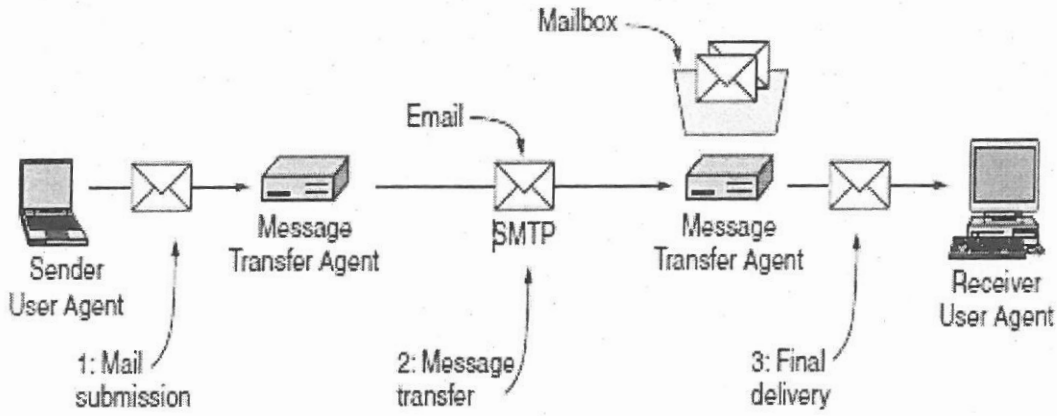


Figure 7-7. Architecture of the email system.

- The architecture of e-mail systems normally consist of two subsystems: the **user agents**, which allow people to read and send e-mail, and the **message transfer agents**, which move the messages from the source to the destination.
- The **user agents** are local programs that provide a command based, menu-based, or graphical method for interacting with the e-mail system.
- The **message transfer agents** are typically system **daemons**, that is, processes that run in the background. Their job is to move e-mail through the system.
- A key idea in e-mail systems is the distinction between the **envelope** and its contents. The envelope encapsulates the message. It contains all the information needed for transporting the message, such as the destination address, priority, and security level, all of which are distinct from the message itself.
- The message transport agents use the envelope for routing, just as the post office does.
- The message inside the envelope consists of two parts: the **header** and the **body**. The header contains control information for the user agents. The body is entirely for the human recipient.