CHAPTER 10

COMPUTER NETWORKS

Syllabus: Computer networks: ISO/OSI stack, LAN technologies (Ethernet, token ring), Flow-and error-control techniques, Routing algorithms, Congestion control, TCP/UDP and sockets, IP(v4), Application-layer protocols (ICMP, DNS, SMTP, POP, FTP, HTTP); Basic concepts of hubs, switches, gateways and routers; Network security: basic concepts of public key and private key cryptography, digital signature, firewalls.

10.1 INTRODUCTION

Computer network is a collection of autonomous devices interconnected via a medium. The medium may be a guided medium, a wireless medium or a satellite communication. To understand data communication, different layered architectures have been presented. All layers execute different protocols to communicate the data successfully from one end to the other. The intermediary devices such as switch, hub, router or gateway help in advancing this communication. Although the security requirements may be different depending upon the application, network security cannot be left aside when studying networks.

10.2 NETWORK

Two or more devices connecting to each other through any medium forms a network. To connect the devices there are two possible ways:

1. **Point-to-point connection:** This provides a dedicated link between the two devices.
2. **Multipoint connection:** This is also known as multi-drop connection. In this case, channel capacity is shared by more than two devices. In general, this is used in practice. All the five examples in Fig. 10.1 are multipoint.

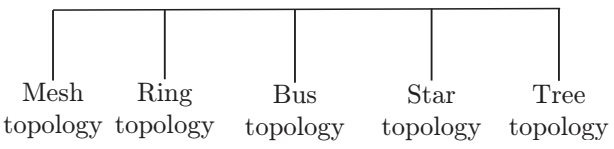


Figure 10.1 | Network topology.

10.2.1 Network Topology

The physical or logical view of interconnection among devices is known as topology.

Ring and mesh topology are examples of peer-to-peer relationship because here all the devices share the link equally. Bus, star and tree topologies are examples of primary—secondary relationship, where one device controls and the other devices have to transmit through it.

10.2.1.1 Bus Topology

In a bus network, all the devices are connected with one cable. The major benefit here is, we require less cable length than star topology and expansion is quite easy with the help of repeaters.

The issues associated with bus topology are as follows:

1. Only one device can send the data at one time. All the devices will listen at that time.
2. The data communication is only in one direction.
3. In a bus topology, if the network shuts down then there is problem in identifying the culprit device.

10.2.1.2 Ring Topology

In a ring topology, each deviceis connected exactly to two devices to form the ring. Repeaters are used to regenerate and retransmit each bit. Data travels around the network in one direction. Data travels in the form of token. Additional components do not affect the performance of the network. Even if the load on the network increases, the performance of a ring topology is better than a bus topology. The problems may be listed as follows:

1. Failure of one computer in the ring may lead to entire communication loss.
2. Network scaling is difficult.

For example, token ring is defined by IEEE 802.5 standard.

10.2.1.3 Star Topology

In a star topology, a hub is placed at the central location and all the devices are connected to the hub. All communication is possible through the hub only. If the hub is active, it may amplify or regenerate the signals. The following are the drawbacks of a star topology:

1. If the central hub fails, no communication is possible.
2. Cabling cost is more.

For example, Ethernet 10 base T is a popular example.

10.2.1.4 Mesh Topology

All the devices are connected through peer-to-peer links. A fully connected mesh will have $n(n-1)/2$ physical channels to connect n devices. The advantage of mesh topology is security and privacy. A dedicated link will eliminate traffic problems, and fault diagnose is easy here. But cabling cost and other hardware required make it difficult to implement in real practice. It is better to use this topology in backbone network and other topologies for further network configuration.

10.2.1.5 Tree Topology

A tree topology maintains the devices connected to a central hub as well as to some secondary hubs, which are again connected to the central hub. It allows an isolated network which prioritizes communication from different computers. It also faces the same problem as in a star topology; failure of central hub will crash the entire network. Also, it has high cabling cost.

10.3 LAN TECHNOLOGIES

LAN (local area network) is an integral part to create a network. There are many LAN technologies such as Ethernet, token ring, token bus, FDDI (fiber distributed data interface) and ATM LAN. Table 10.1 shows the comparison of Ethernet, token bus and token ring.

10.3.1 Ethernet

Xerox Corporation, Digital Equipment Corporation and Intel Corporation developed Ethernet LAN technology in 1976. Ethernet is based on the IEEE 802.3 specification. It is a linear-bus logical topology. Ethernet is the most widely used LAN technology in the world. It has passed four generations: Standard Ethernet (10 t Mbps), Fast Ethernet (100 Mbps), Gigabit Ethernet (1 Gbps) and Ten-Gigabit Ethernet (10 Gbps). Earlier Ethernet designed were of two types: Thicknet (thick coaxial main trunk cable of 10 mm and Thinnet (thin coaxial cable: RG-58 of 5 mm). In 1990, unshielded twisted-pair (10Base-T) Ethernet came into existence. Ethernet uses

Table 10.1 | Comparison of Ethernet, token bus and token ring

Attribute	Ethernet	Token Bus	Token Ring
Physical Topology	Linear	Linear	Star
Logical Topology	None	Ring	Ring
Connection	Random	By token	By token
Node Addition	Node added anywhere and anytime	Distributed algorithms are responsible for node addition	Between two specified nodes
Cable Used	Twisted pair, co-axial and fibre optic	Co-axial	Twisted pair and fibre optic
Cable Length	50–2000 m	200–500 m	50–1000 m
Frequency	10–100 Mbps	10 Mbps	4–100 Mbps
Frame Structure	1500 byte	8191 bytes	5000 bytes
IEEE Standard	802.3	802.4	802.5
Maintenance	No central maintenance	By distributed algorithms	By a designated monitor node
Performance	Immediately transmitted by the nodes, heavy traffic can reduce the effectiveness of transmission	Nodes must wait for the token if no other node is transmitting. During heavy traffic, token passing provides fair access to all nodes	Nodes must wait for token even if no other node is transmitting. During heavy traffic, token passing provides fair access to all nodes
Maximum Delay before Transmitting	None	Bounded, depending on distance spanned and number of nodes	Bounded, depending on distance spanned and number of nodes

Carrier-Sense Multiple Access with Collision Detection (CSMA/CD) access control scheme. The drawback of this topology is that if one of the links between the two adjacent nodes fails, the whole network fails.

10.3.2 Token Bus

Token bus is a bus (physical view) ring (logical view) topology. In token bus, nodes are connected linearly. However, they make a logical ring, as each node knows the address of its successor.

10.3.3 Token Ring

Token ring is a star (physical view) ring (logical view) topology. The hub acts as a connector. The wiring inside the hub makes the ring; the stations are connected to this ring through the two wire connections. It is more efficient; if a link goes down, it will bypass the hub and operate the other nodes. It also improves the scalability of the network.

In early token release,

$$\text{Throughput for single station or } N \text{ stations} = \frac{\text{Data}}{\text{Transmission time} + (\text{Ring latency}/\text{Number of stations})}$$

In delayed token release,

$$\text{Throughput for single station} = \frac{\text{Data}}{\text{Transmission time} + \text{Ring latency} + (\text{Ring latency}/\text{Number of stations})}$$

$$\text{Throughput for } N \text{ stations} = \frac{\text{Data}}{\text{Ring latency} + (\text{Ring latency}/\text{Number of stations})}$$

10.4 ISO/OSI STACK

There are two reference models based on the network architectures. One is the International Standards Organization/Open Systems Interconnection (Reference Model 1984) (ISO/OSI) model and other is the Transmission Control Protocol/Internet Protocol (TCP/IP) model. The layered architecture of both the models has been compared in Fig. 10.2.

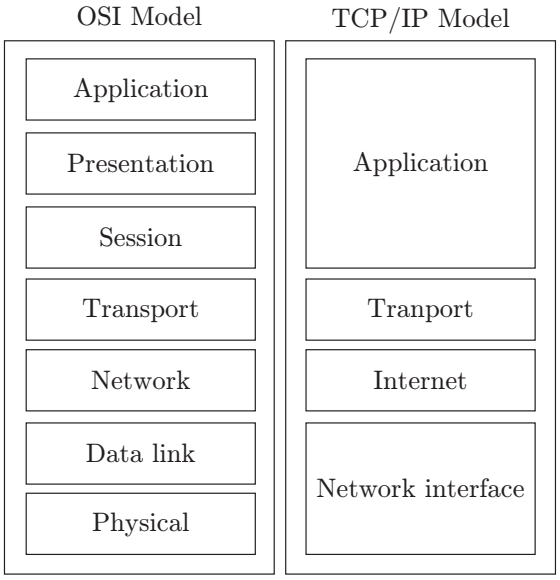


Figure 10.2 OSI and TCP/IP model.

The ISO/OSI model has seven layers while TCP/IP has only four layers. Session and presentation layers are completely missing. Characteristics of the session layer are provided by the transport layer, and the application layer bears the accountability of the presentation layer. Host to network is the lowest layer in the TCP/IP model and its duty is to send IP packets to the network. In the ISO/OSI model, the network layer provides connection-oriented as well as connectionless services, but the TCP/IP model provides only connectionless services.

If M is a message and H is the header that is added at every layer and N layers are present in hierarchy, then the fraction of header that is passed in the total content is calculated as follows:

$$\text{Fraction of data} = \frac{M}{NH + M}$$

10.4.1 ISO/OSI Model

10.4.1.1 Layer 1: Physical Layer

The major responsibilities of physical layer are transmission of raw bit stream and to form the physical interface between two communicating devices. The conversion of analog to digital and digital to analog is performed at this layer.

The following are some issues listed which may create problems before/during transmission:

1. Compatibility of mechanical and electrical interfaces
2. Working of physical transmission media
3. Deciding on the number of bits per second to be sent
4. Finding out whether transmission is simplex or duplex
5. Establishing and terminating the initial communication when both sender and receiver are finished

$$\text{Transmission time} = \frac{\text{Message size (bits)}}{\text{Bandwidth (bits/s)}}$$

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

Problem 10.1: Message size = 1 Kb

$$\text{Bandwidth} = 1 \text{ Mbps}$$

$$\text{Transmission time} = \frac{1 \text{ Kb}}{1 \text{ Mbps}} = \frac{10^3 \times 2^3 \text{bits}}{10^6 \text{bits/s}} = 8 \times 10^{-3} \text{ s}$$

If link utilisation is 50%, what is the relation between transmission time and propagation time?

Solution:

$$\text{Link utilization of sender} = \frac{\text{Transmission time}}{\text{Transmission time} + 2 \times \text{Propagation time}}$$

$$\frac{1}{2} = \frac{\text{Transmission time}}{\text{Transmission time} + 2 \times \text{Propagation time}}$$

Transmission time + 2 × Propagation time
= 2 × Transmission time

Therefore, Transmission time = 2 × Propagation time

$$\text{Transmission time} = 2 \times \text{Propagation time}$$

or $$\text{Transmission time} = \text{Round-trip time}$$

Let L be the message, B the bandwidth and R the round-trip time (RTT),

$$\text{Link utilization of sender} = \frac{L/B}{(L/B) + R}$$

$$\eta = \frac{L}{L + BR}$$

In the above expression,

1. if L = BR, $\eta = 50\%$
2. if $L > BR$, $\eta > 50\%$
3. if $L < BR$, $\eta < 50\%$
4. if $L >>> BR$, $\eta \simeq 100\%$
5. if $L <<< BR$, $\eta \simeq 0\%$

10.4.1.2 Layer 2: Data Link Layer

Data link layer provides reliable transfer of information between two adjacent nodes. Also, it provides frame-level error control and flow control. It provides

communication between machines on the same network. Communication between two devices can be simplex, half-duplex, or full-duplex. In simplex, the communication is unidirectional. In half-duplex, each device can both transmit and receive, but not at the same time. In full-duplex, both devices can transmit and receive simultaneously.

This layer is responsible for encoding and decoding i.e. converting bits to signals at sender site and recovering bits from received signals at receiver side; frame creation i.e. deciding a minimum unit for sending bits; error detection and/or correction of frames through parity or CRC and flow control using ARQ, sliding WINDOW etc. The functionality of data link layer is as follows:

1. **Encoding:** Signals propagate over a physical medium – (1) modulate electromagnetic waves (varying voltage); (2) encode binary data onto signals (e.g., 0 as low signal or non-return to zero, NRZ, and 1 as high signal or non-return to zero inverted, NRZI); make a transition from current signal to encode a 1 or stay at the current signal to encode a 0;(3) Manchester (transmit XOR of the NRZ-encoded data and the clock only 50% efficient).
   In Manchester encoding, a clock signal and data signal are mixed together by XORing operation. The clock makes a clock transition in every bit time, so it runs at twice the bit rate. When it is XORed with 0 then it makes low-to-high transition, it acts as a clock and when it is XORed with 1 then it makes high-to-low transition, it acts as a data signal.
2. **Framing:** The basic data unit at the date link layer is called a 'frame' which is a collection of bits in sequence boundary. In order to mark boundaries of frame starting and ending characters are used.
3. **Flow control:** It is a mechanism which informs the sender about the amount of data transmission before receiving an acknowledgement from the receiver. As the receiving device has limited speed for processing the incoming data and limited memory to store data, so it informs the sending device by sending few frames and stop. The receiving device has a buffer, a block of memory, for storing extra incoming data before processing.
4. **Error control:** It is a mechanism which informs the sender about the retransmission of the damaged and lost frames during transmission. It is a method of error detection and error correction. Automatic repeat request (ARQ) is a process in which whenever an error is detected, the receiving device sends the request for retransmission to sender.
5. **Techniques of flow and error control:**
   - *Stop-and-wait automatic repeat request:* In this protocol, the sender starts the timer and keeps the copy of the sent frame. If the timer expires and there is no acknowledgement (ACK) for the sent frame, the frame is resent, the copy is held and the timer is restarted. For the corrupted and lost ACK frame, sequence numbers can be used. In the data frame, a field is added for the sequence number. The sequence numbers are based on modulo-2 arithmetic. This protocol is also having acknowledgement numbers, which specifies the sequence number of the next frame expected by the receiver. A data frame uses a sequence number and an ACK frame uses an acknowledgement number. The control variable of sender keeps the sequence number for the next frame to be sent (0 or 1). The control variable of receiver keeps the number of the next frame expected. When a frame is sent, the value of the control variable of sender is incremented. When a frame is received, the value of the control variable of receiveris incremented. The stop-and-wait ARQ protocol is very inefficient if the channel is thick (large bandwidth) and long (long round-trip delay). Other drawback of this protocol is that it does not support pipelining, as it does not support multiple frames.Pipelining helps in improving the efficiency of the transmission, if the number of bits in transition is large with respect to the bandwidth-delay product.
     For stop-and-wait ARQ,

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

$$\text{Propagation delay} = \frac{\text{Distance of the link}}{\text{Velocity}}$$

Link utilisation of sender or throughput is given by

$$\eta = \frac{\text{Transmission time}}{\text{Transmission time} + 2 \times \text{Propagation delay}}$$

   - *Go-back-N automatic repeat request:* This protocol helps in improving the efficiency of transmission by filling the pipe. It supports multiple frames during wait for acknowledgement. The sequence numbers are modulo 2^m, where m is the size of the sequence number field in bits. Sliding window defines the range of sequence numbers related to the sender and receiver. When the timer expires, the sender resends all outstanding frames. Stop-and-wait ARQ is a special case of Go-Back-N ARQ in which the size of the send window is 1. It supports one receiver window size. This protocol is very inefficient for a noisy link. In noisy link, frames are resending again and again, which uses bandwidth and slow down the transmission. For Go-Back-N ARQ,

     Sender window size $< 2m$
     Maximum sequence number $= 2m - 1$
     where m is the number of segment bits.

If maximum sequence number is s, then the number of sequence bits = log (s+1)

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

$$\text{Propagation delay} = \frac{\text{Distance}}{\text{Velocity}}$$

Link utilisation of sender or throughput is given by

$$\eta = \frac{\text{Transmission time}}{\text{Transmission time} + 2 \times \text{Propagation delay}}$$

$$\text{Number of frames (Window size)} = \frac{\text{Total bits}}{\text{Frame size}}$$

- *Selective repeat automatic repeat request:* In this protocol, the damaged frame is resent in the network. It is efficient for noisy links, but it requires complex processing at the receiver end.

  Sender window size
  = Receiver window size $\leq 2^m - 1$

  If Q is the size of the window, then the number of sequence bits = $\log_2 Q + 1$

$$\text{Number of frames (Window size)} = \frac{\text{Total bits}}{\text{Frame size}}$$

Problem 10.2: Calculate the link utilisation for stop-and-wait flow control mechanism if the frame size is 4800 bits, bit rate is 9600 bps and distance between devices is 2000 km. Given propagation speed is 200000 km/s.

Solution:

$$\eta = \frac{4800/9600}{(4800/9600) + 2 \times (2000/200000)} = 0.96$$

6. **Parity bits:** Append a single parity bit to a sequence of bits
   - If using 'odd' parity, the parity bit is calculated as making the total number of 1's in the bit sequence odd;
   - If using 'even' parity, the parity bit makes the total number of 1's in the bit sequence even

   For example, if $-Q$ is for even parity, what's the parity bit for 00010101? The problem with parity bit is that it only detects when there are an odd number of bit errors.
7. **Polynomial codes:** It can detect errors on large chunks of data; has low overhead; is more robust than parity bit; and requires the use of a code polynomial.
8. **Cyclic Redundancy Check (CRC):** Example of a polynomial code

   Procedure:
   - Let r be the degree of the code polynomial. Append r zero bits to the end of the transmitted bit string. Call the entire bit string $S(x)$.
   - Divide $S(x)$ by the code polynomial using modulo-2 division.
   - Subtract the remainder from $S(x)$ using modulo-2 subtraction.

   The result is the checksummed message.
9. **Decoding a CRC procedure:**
   - Let n be the length of the checksummed message in bits.
   - Divide the checksummed message by the code polynomial using modulo-2 division. If the remainder is zero, there is no error detected.
10. **Choosing a CRC polynomial:** The longer the polynomial, the smaller the probability of undetected error.

Problem 10.3: If the frame is 1101011011 and generator is $x^4 + x + 1$, what would be the transmitted frame?

Solution: The polynomial $x^4 + x + 1$ corresponds to divisor 10011($k = 5$ bits)

Data word (1101011011) of N = 10 bits is augmented with $(k - 1)$ zero's.

Dividend = 11010110110000

```
              110000101
         ┌──────────────
   10011 ) 11010110110000
           10011
           ─────
           010011
            10011
           ──────
           0000010110
                10011
               ──────
                0010100
                 10011
                ──────
                 001110
```

After dividing the message 1101011011 by 10011 the remainder is 1110, which is CRC. The transmitted data is data + CRC, which is 1101011011 + 1110 = 11010110111110.

Data link layer is divided into two sublayers:

1. **Multiple access control sublayer:** It provides controlled access to shared transmission media.
2. **Logical link control sublayer:** It is responsible for error and flow control.

When multiple users share a common communication link, multiple access protocols are used to coordinate access to common link (Fig. 10.3).

1. **Random Access Protocols:** The following are the different random access protocols used for accessing the shared transmission channel:
   - *Pure ALOHA:* It says that whenever a station is having the data, they can send immediately. The time at which the collision occurs is called vulnerable time.

$$T_p = \text{Maximum propagation time} = \frac{\text{Distance between two stations}}{\text{Velocity}}$$

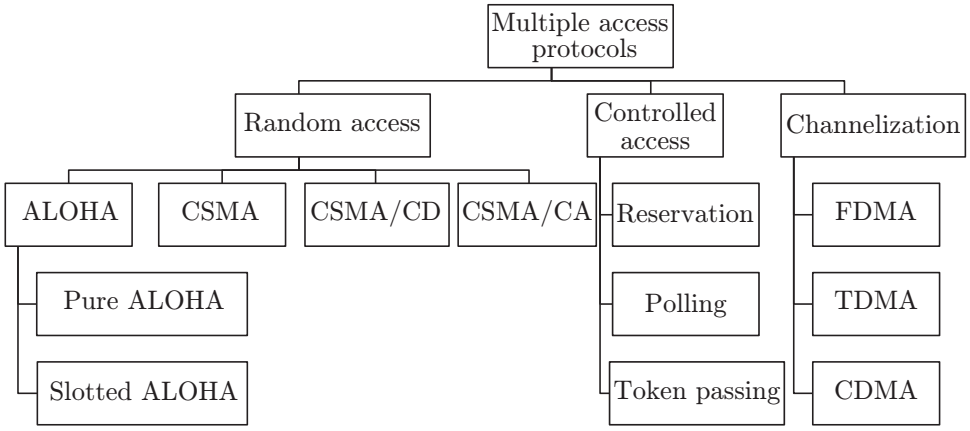


Figure 10.3 | Multiple access protocols.

Suppose T_{fr} is the average transmission time for a frame, then

$$T_{fr} = \frac{\text{Frame size}}{\text{Bandwidth}} = G$$

$$\text{Throughput } (S) = G \times e^{-2G}$$

$$\text{Vulnerable time} = 2 \times T_{fr}$$

$$S_{\max} = 18.4\%$$

- *Slotted ALOHA:* It says that if stations are ready with the data, they have to wait for the required time slot and can transmit data exactly at that timeslot.

$$\text{Throughput } (S) = G \times e^{-G}$$

$$\text{Vulnerable time} = T_{fr}$$

$$S_{\max} = 36.8\%$$

- *CSMA (Carrier Sense Multiple Access):* If a station is ready with the data, it senses the channel, and if channel found idle, data is transmitted, otherwise the station has to wait for random amount of time.

10.4.1.3 Layer 3: Network Layer

The network layer is responsible for host-to-host delivery and path selection between endsystems (routing). The fragmentation, reassembly and translation between different network types are also performed at this layer. In other words, communication between nodes is possible in different networks through this layer.

Packet delivery can be accomplished by using either a connection-oriented or a connectionless network service. In a connection-oriented protocol, the connection is established before sending the packets so route is established before and all the packets have to follow that route. Example: Frame relay and ATM uses this service.

In connectionless protocols, the network layer protocol treats each packet independently. The packets in a message may or may not follow the same path to their destination. For example, Internet uses this type of service.

Switching can be broadly divided into three categories: circuit switching, packet switching and message switching, as shown in Table 10.2.

Table 10.2 | Comparison of circuit, message and packet switching

Attribute	Circuit	Message	Packet
Dedicated Physical Path	Yes	No	No
Bandwidth Available	Fixed		Dynamic
Route Selection	Static	Dynamic (per message)	Dynamic (per packet)
Potentially Wasted Bandwidth	Yes	No	No
Stored and Forward Transmission	No	Stored	Queued not stored
Transmission Length	Unlimited	Maximum length	No maximum length
Same Route Follows	Yes	No	No

(*Continued*)

Table 10.2 Continued

Attribute	Circuit	Message	Packet
Packets Arrive in Order	Yes		No
Call Setup	Required	Not Required	Not required
Congestion Route Blocking	At setup time, if user busy	No message blocking	On every packet
Possible Reordering	No	No	Yes
Response to Link Failure	Data loss	Rerouting/Retransmission	Rerouting/Retrans-mission
Message Delivery	Guaranteed	Depends on the network	Depends on the network
Delivery Time	Negligible	Long	Short
Path Establishment	Switch path for entire connection time	For each message	For each packet
Charging	Per minute	Per message	Per packet

The **Internet** is a global system of computer networks that are interconnected worldwide and all use the standard Internet protocol suite (TCP/IP) for linking.

1. **Internet as a Datagram Network:** The Internet, at the network layer, is a packet-switched network. Switching can be generally divided into three broad categories: circuit switching, packet switching, and message switching. Packet switching uses either the virtual circuit approach or the datagram approach.

   The Internet chooses the datagram approach to switching in the network layer, and uses the universal addresses defined in the network layer to route packets from the source to the destination. Switching at the network layer in the Internet uses the datagram approach to packet switching.
2. **Why Internet Uses Connectionless Network?** Delivery of a packet can be accomplished by using either a connection-oriented through TCP or a connectionless network service through UDP (see Table 10.3). In a connection-oriented service, the source has to make a connection with the destination before sending a data packet. Only after establishing connection, a sequence of packets from source to the destination can be sent on the same path that is established before in a sequential order. The connection is terminated only when all the packets of a particular message have been successfully. But the communication at the network layer in the Internet is connectionless. The reason is that Internet is made of so many heterogeneous networks that it is almost impossible to create a connection between every source and destination pair without knowing the nature of the networks in advance.

Table 10.3 Comparison between TCP and UDP

Attribute	TCP	UDP
Connection Management	Connection oriented	Connectionless
End-to-End Connection	Dedicated connection	No dedicated connection
Reliability	Reliable	Unreliable
Transmission	Byte oriented	Message oriented
Acknowledgement	Yes	No
Retransmission	Automatically	If needed
Congestion Control	Yes	No
Flow Control	Yes	No
Fault Tolerance	No	No
Data Delivery	Strictly ordered	Unordered
Security	Yes	Yes
Overhead	Low	Very low
Transmission Speed	High	Very high
Data Quantity Suitability	Small to very large amount of data	Small to moderate amount of data

10.5 ROUTING ALGORITHMS

When the router receives a packet, which route this packet should follow to reach to destination is an important concern. This is one of the major responsibilities of network

layer. This decision is taken by router on the basis of the routing table maintained by it. The algorithm which decides the suitable route is known as routing algorithm. The desirable properties of any routing algorithm are correctness, fairness, stability, robustness and optimality.

These algorithms can be broadly divided into two categories:

1. **Adaptive algorithms:** The dynamic routing decision depends on the topology and traffic. Furthermore, adaptive algorithms have been divided into three forms:
   - ***Centralised:*** The decision is taken on the basis of global information and this is performed by a centralised node.
   - ***Isolated:*** The routing decision is taken based on local information. Generally, routers do not share information with their neighbours.
   - ***Distributed:*** A combination of local and global information.
2. **Non-adaptive algorithms:** The static routing decision is taken in advance and it is downloaded by the routers, that is, never change once initial route has been selected.

The properties of non-adaptive routing algorithms are as follows:

1. **Optimality principal:** It states that "if router J is on the optimal path from router I to router K, then the optimal path from J to K also falls along the same route". In other words, suppose r_1 is the route from I to J and r_2 is rest of the route. Then, if any route is better than r_2, it could have improved the overall optimal route. Hence, r_1r_2 is optimal.
2. **Sink tree:** A set of all optimal routes from any source to a fixed destination form a tree called sink tree. Sink trees may be more than one with the same path length. The concern of sink tree here is to help routers find the best path.

In addition to adaptive and non-adaptive categorisation, routing algorithm can be simply categorised into the following:

1. Static routing (shortest path, flooding)
2. Flow-based routing
3. Dynamic routing (distance vector, link state routing)
4. Hierarchical routing
5. Routing for mobile hosts
6. Broadcast routing
7. Multicast routing

These are explained as follows:

1. **Shortest path routing:** This non-adaptive approach is based on the simplest and most widely used principle. Each node is treated as a router and each arc as communication link. To find a path between a pair of routers, the shortest path is chosen. The shortest path is chosen based on the number of hops or geographical distance in kilometres. Dijkstra's and Bellman–Ford's algorithm are the most famous shortest path algorithms.

Example 10.1

Flooding: This is again a non-adaptive algorithm and it sends a copy of the packet to every outgoing line except the line on which it was received. This guarantees the packet delivery to destination but a large number of packet copies will be generated. Sometimes this count approaches to infinity and the only solution is to discard the packet using any of the following approach:

(a) Using a hop counter to avoid forwarding of packets as number of hops reaches the diameter of the network.
(b) Keeping track of flooded packets.
(c) Selective forwarding by forwarding only those relevant packets which approaches to the right destination.

To avoid looping, a sequence number may be added to each packet's header. This helps in discarding those packets whose sequence number is lower than the one already received.

Note: Although flooding is inefficient in most applications, an exception may be in the case of military application where large number of routers are placed and robustness is highly desirable.

2. **Flow-based routing:** This is a non-adaptive algorithm which uses topology and traffic condition for deciding the route. If traffic on some route is more than average, then the route should be avoided to achieve optimal path.

   If line capacity and flow is given, delay can be determined easily using the following formula:

$$T = \frac{1}{\mu C - \lambda}$$

   where $1/\mu$ is mean packet size in bits, λ is the mean number of packets arrived per second and C is the line capacity in Kbps.

Example 10.2

Distance Vector/Distributed Bellman–Ford/ Ford–Fulk-erson Routing Algorithm: This is one of the popular examples of dynamic routing algorithm. Each router maintains a table (called vector) which helps in finding the best-known distance to any destination. It also indicates preferred outgoing line to be used to reach the destination. The performance metric can be the number of hops, time delay or number of packets in the queue.

Issues:

(a) Slowness in converging to the right answer and this problem is well known as count to infinity (can be solved using split-horizon algorithm).
(b) Line bandwidth should be a metric when choosing root.

Whenever a packet comes to a router, the neighbouring router will give their routing table and a new vector table is created at that router.

Example 10.3

Consider a network shown in Fig. 10.4:

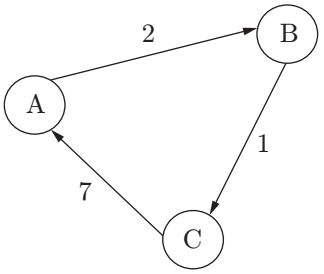


Figure 10.4

Step 1: Initialise cost of direct links and set to ∞cost from neighbours.

Node A table

		Cost to		
		A		C
From	A	0	2	7
	B	∞	∞	∞
	C	∞	∞	∞

Node B table

		Cost to		
		A	B	C
From	A	∞	∞	∞
	B	2	0	1
	C	∞	∞	∞

Node C table

		Cost to		
		A	B	C
From	A	∞	∞	∞
	B	∞	∞	∞
	C	7	1	0

Step 2: Each node periodically sends its own distance vector (DV) to neighbours. When node A receives DV from neighbour B, it keeps it and updates its own DV as follows:

$$D_A(\mathrm{B}) = \min_v\{\, C(x,v) + D_v(\mathrm{B})\}$$

Node A updated table after receiving DV from node B and node C is:

$$D_A(\mathrm{B}) = \min\{2 + 0{,}7 + 1\} = 2 \text{ and}$$
$$D_A(\mathrm{C}) = \min\{2 + 1{,}7 + 0\} = 3$$

Node A table

		Cost to		
		A	B	C
From	A	0	2	3
	B	2	0	1
	C	7	1	0

Node B table

		Cost to		
		A	B	C
From	A	0	2	7
	B	2	0	1
	C	7	1	0

Node C table

		Cost to		
		A	B	C
From	A	0	2	7
	B	3	0	1
	C	3	1	0

Step 3: In similar fashion, algorithm proceeds until all nodes have updated tables.

Node A table

		Cost to		
		A	B	C
From	A	0	2	3
	B	2	0	1
	C	3	1	0

Node B table

		Cost to		
		A	B	C
From	A	0	2	3
	B	2	0	1
	C	3	1	0

Node C table

		Cost to		
		A	B	C
From	A	0	2	3
	B	2	0	1
	C	3	1	0

3. **Link state routing:** This is simply a modern replacement of distance vector routing. The steps of the algorithm are as follows:
   - Each router discovers the neighbours for their network addresses.
   - Measure delay or cost to each of these neighbours.
   - Construct a packet including network address and delays of all neighbours.
   - Send it to all routers.
   - Find the shortest path to all routers (Dijkstra's algorithm can be used).

Example 10.4

OSPF protocol (used in Internet) uses the link state algorithm: IS-IS (intermediate system–intermediate system) is another example used in Internet backbones and in some digital cellular systems.

4. **Hierarchical routing:** In the situation of telephone networks, all above routing algorithms fail because the size of the routing table is too large here. In this routing, routers are divided (placed) into different regions. A router will have the knowledge of other routers in its own region but unaware about the internal structure of other regions. This will reduce the size of the routing table.
5. **Broadcast and multicasting routing:** Broadcasting means sending packets to all other hosts in the network, whereas multicasting refers to sending packets to a specific group or a fixed number of hosts.

10.6 NETWORK LAYER PROTOCOLS

In the Internet model, or the TCP/IP suite, there are five main network layer protocols: ARP, RARP, IP, ICMP and IGMP (Fig. 10.5).

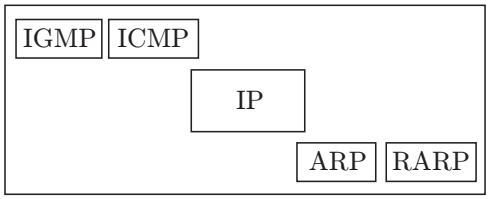


Figure 10.5 Network protocols.

The main protocol in this layer is IP. It is responsible for host to host delivery of packets from a source to destination. IP needs services of other protocols for better network performance. IP needs ARP to find MAC address of the next hop. As IP is an unreliable protocol, it needs ICMP (Internet Control Message Protocol) to handle unusual situations and errors. IGMP (Internet Group Message Protocol) is used for multicast delivery.

10.6.1 Internet Protocol (IPv4)

Internet Protocol is a layer-3 protocol of network layer of OSI model. It takes data segments from layer-4 transport layer and divides it into packets. Thus, it encapsulates data units received from the above layer and adds its own header information (Fig. 10.6).

Maximum size of IP header = 60 bytes

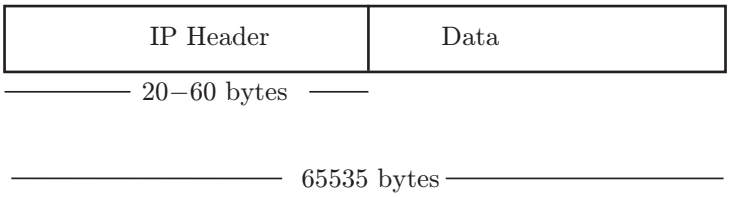
Minimum size of IP header = 20 bytes

If the size of header is 32 bytes in IP, calculate the number of option bytes.

Option bytes = 32 − 20 = 12 bytes

IP header details are as follows:

1. **Version:** Version number of Internet Protocol is 4 (e.g. IPv4).
2. **IHL:** Internet header length indicates the size of header available in the packet.
3. **TOS:** Type of service that is provided by the router to the packets such as minimum delay or cost.
4. **Total length:** Length of the entire IP packet (including IP header and IP payload).
5. **Identification:** If IP packet size is greater than the maximum transmission unit (MTU), it has to be fragmented during the transmission by the router, then all the fragments of the packet contain same identification number to identify original IP packet they belong to.
6. **Flags:** If IP packet is too large, these 'flags' tell if they can be fragmented or not. In 3-bit flag, the MSB is



Version (4 bits)	IHL (4 bits)	TOS (8 bits)	Total length (16 bits)	
Identification (Fragment ID) (16 bits)			Flags (3 bits)	Fragmentation offset (13 bits)
Time to live (8 bits)		Protocol (8 bits)	Header checksum (16 bits)	
32-Bit source address				
32-Bit destination address				
Options (if any, variable length, padded with 0's, 40 bytes maximum length)				

Figure 10.6 | IPv4 packet header.

always set to '0'. The next bit is DF (do not fragment). If DF = 0, fragmentation can be done if required and buffered at the router of the receiver until all fragment comes, and if DF = 1, fragmentation should not be done. The third bit is MF (more fragment). If MF = 1, then datagram is not the last fragment. If MF = 0, then datagram is the last fragment.

7. **Fragment offset:** This offset tells the exact position of the fragment in the original IP packet.
8. **Time to live:** It controls the maximum number of routers visited by the datagram. To avoid looping in the network, every datagram is sent with some-time-to-live(TTL) value set. Each router receiving the datagram decreases TTL by 1 and when it becomes 0, the datagram is discarded.
9. **Protocol:** It tells the higher-level protocol which uses the service of the IP layer. For example, protocol number for ICMP is 1, IGMP is 2, TCP is 6 and UDP is 17.
10. **Header checksum:** This field stores checksum value of the entire header excluding data which is used to check if the packet has been received error-free.
11. **Source address:** 32-Bit address of the sender of the packet.
12. **Destination address:** 32-Bit address of the receiver of the packet.
13. **Options:** These options may contain values for various options such as strict source routing, security, record route, time stamp, etc.

Problem 10.4: If the total length bits are 0000000000 111111 and header length is 1001, calculate the size of the packet, header and payload.

Solution:

(a) Packet size = Decimal equivalent of 00000000 00111111 = 63 bytes
(b) Header size (1001) = $9 \times 4 = 36$ bytes
(c) Packet size = Header + Payload

Payload = Packet size − Header = 63 − 36
= 27 bytes

Problem 10.5: Suppose a router receives an IP packet containing 600 data bytes and has to follow a packet maximum transferable unit of 200 bytes. Assume that the IP header is 20 bytes long; specify the relevant values in each fragment header.

Solution: IP packet = 600 bytes
MTU = 200 bytes

IP header = 20 bytes

Maximum possible data length per fragment = 200 − 20 = 180 bytes

Data length of each fragment must be a multiple of 8 bytes so 22 × 8 = 176 bytes

Data packet must be divided into the following four frames:

(176 + 20) + (176 + 20) + (176 + 20) + (72 + 20) = 680

	Length	ID	MF	Fragment Offset
Original Packet	620 bytes	X	0	0
Fragment 1	196 bytes	Z	1	0
Fragment 2	196 bytes	Z	1	22
Fragment 3	196 bytes	Z	1	44
Fragment 4	92 bytes	Z	0	66

10.6.1.1 IPv4 Addresses

An **IPv4** address is a 32-bit address that can find the device on the Internet uniquely and universally. These addresses are unique, that is, these define only one connection by the device to the Internet. The total number of addresses used by this protocol which is called as address space is 2^n where n is the total number of bits. As IPv4 uses 32-bit addresses, the address space of this protocol is 2^{32}.

In IPv4, addresses are 32-bit binary numbers. However, for ease of use of people, theses binary patters are represented as dotted decimals. Therefore, there are two notations available to denote IPv4 addresses: binary and dotted decimal.

1. **Binary notation:** In this notation, IPv4 addresses are represented as 32 bits where each octet is said to be a byte. Therefore, the IPv4 address is usually said to be the 4-byte address. The example for this notation is as follows:

   01111101 10000011 00000110 00000001

2. **Dotted-decimal notation:** In this notation, each byte (8 bits) of 32-bit binary address, known as octet is separated with a dot, and then the binary number is converted into its decimal equivalent. The example for this notation is as follows:

   11000000 10101000 00001010 00001010
   is equivalent to 192.168.10.10

Classful Addressing

The architecture used by IPv4 is classful addressing where the addresses are divided into five classes: A, B, C, D and E. The first few bits reveal the class of address when the address is in binary and first byte reveals the class of address when the address is in dotted decimal notation. This architecture is called classful addressing (Table 10.4).

Table 10.4 Classful addressing architecture of IPv4

	Leading Bits	Value Range	Starting Address	Ending Address
Class A	0	0–126	0.0.0.0	127.255.255.255
Class B	10	128–191	128.0.0.0	191.255.255.255
Class C	110	192–223	192.0.0.0	223.255.255.255
Class D	1110	224–239	224.0.0.0	239.255.255.255
Class E	1111	240+	240.0.0.0	255.255.255.255

Note: 127 reserved for loopback address.

The addresses of class A, B, C are unicast, class D addresses are multicast and class E addresses are reserved. The IP address in class A, B and C is divided into **netid** and **hostid**. In class A, one byte defines the netid and the other three bytes define the hostid. In class B, two bytes define the netid, while the other two bytes define the hostid. In class C, three bytes define the netid and one byte defines the hostid.

Mask: The length of the netid and hostid (in bits) is predetermined in classful addressing but we can also use a mask (also called the default mask) which is a 32-bit number made of contiguous 1's. The subnet mask is compared to the IP address from left to right, bit for bit. The 1's in the subnet mask represent the network portion and 0's represent the host portion. The subnet mask is created by placing a binary 1 in each bit position that represents the network portion and placing a binary 0 in each bit position that represents the host portion.

The subnet mask assigned along with IP address signifies which part of the IP address is network and which part is host.

There is a flaw in this type of architecture, that is, each class is divided into fixed number of blocks, and a lot of addresses are wasted as blocks A and B addresses are too large to consume, block C addresses are small in number, class D addresses are reserved for multicasting and class E addresses are reserved for future, which is another wastage of addresses. Therefore, these address scheme architecture is almost obsolete and leads to an introduction of classless addressing scheme as if there are no address classes.

Classless Addressing

In classless addressing, the addresses are granted in a block and the number of addresses in the block depends

upon the addresses needed by the entity. The addresses in the block must be contiguous, the first address must be evenly divisible by the total number of addresses and the number of addresses in a block must be power of 2. Mask in classless addressing can take the value in the range of 0 to 32. Classless Inter-Domain Routing provides the flexibility of borrowing bits of host part of the IP address and using them as smaller sub-networks called subnet. This process is known as **subnetting**. The addresses can be defined in IPv4 as a.b.c.d/n, where a.b.c.d defines one address of the block.

1. The first address in the block can be found by setting the rightmost 32 $-n$ bits to Os in the binary notation.
2. The last address in the block can be found by setting the 32 $-n$ rightmost bits in the binary notation of the address to Is.
3. The number of addresses in the block is the difference between the first and the last address,that is, 2^{32-n}.

Problem 10.6: Determine the subnet identifier, broadcast address and number of valid host addresses having a host with IP address of 196.142.4.29/24.

Solution:

Subnet identifier: 196.142.4.0

Broadcast address: 196.142.4.255

Number of valid host addresses: 254

The subnet mask of /24 in CIDR notation corresponds to 255.255.255.0. The above subnet mask has last eight bits set to zero (32 − 24 = 8), which means that we have 2^8 IP addresses available. Total number of valid hosts in a network is obtained by subtracting two addresses: subnet address and broadcast address $2^8 - 2 = 256 - 2 = 254$.

Problem 10.7: If the IP address of a system is 131.121.61.189, calculate the netid, first host, last host and directed broadcast address.

Solution:

IP address (class B)	131.121.61.189
Net mask	255.255.0.0
Net id	131.121.0.0
First host	131.121.0.1
Directed broadcast address (All host bits 1)	131.121.255.255

Problem 10.8: In class B, if subnet mask is 255.255.240.0, find the number of subnets and host in each subnet.

Solution:

11111111	11111111	1111	0000000
		0000	
Netid		Subnet bits	Host bits

Number of subnets = $2^4 - 2 = 14$ subnets

Number of hosts in each subnet = $2^{12} - 2$ = 4094 subnets

Problem 10.9: If IP address of a system is 199.11.171.189 and subnet mask is 255.255.255.224, calculate the subnet id.

Solution:

IP address	199.11.171.189	
Subnet mask	255.255.255.224	
Subnet id	199.11.171.160	
160 is equivalent to	101	00000
	Subnet Bits	Host Bits

Number of subnets = $2^3 - 2 = 6$

Number of hosts = $2^5 - 2 = 30$

First subnet id is 199.11.171.32 (001 00000).

Second subnet id is 199.11.171.64 (010 00000).

Last subnet id is 199.11.171.192 (110 00000).

First host of first subnet is 199.11.171.33 (001 00001).

Last host of last subnet is 199.11.171.222 (110 11110).

Supernetting is a part of classless addressing. In classless addressing, the addresses should be contiguous in a block. The first address should be exactly divisible by the number of addresses in a block. In supernet, bits are borrowed from netid.

Rules of supernetting:

1. The number of blocks must be power of 2.
2. The blocks must be continuous in the address space.
3. The third octet of the first address in the superblock must be exactly divisible by the number of blocks.

Problem 10.10: A company needs 1000 addresses, which of the following set of class C block can be used to form a supernet?

(a) 198.47.32.0, 198.47.33.0, 198.47.34.0
(b) 198.47.31.0, 198.47.32.0, 198.47.33.0, 198.47.34.0
(c) 198.47.32.0, 198.47.42.0, 198.47.52.0, 198.47.62.0
(d) 198.47.32.0, 198.47.33.0, 198.47.34.0, 198.47.35.0

Solution: (d)

(a) Not in power of 2 or blocks are 3.
(b) Third octet of first address is not divisible by 4.
(c) Blocks are not contiguous.

Problem 10.11: Which of the following can be the beginning address of a block that contains 16 addresses?

(a) 205.16.37.32
(b) 190.16.42.44
(c) 17.17.33.82
(d) 123.45.24.52

Solution:

(a) 32 is divisible by 16.

10.6.2 ICMP

As IP is a connectionless and unreliable protocol, it cannot report errors, so it takes help of ICMP to communicate updates or error information to other intermediate routers, devices or hosts.

Each ICMP message contains three fields: Type, Code and Checksum (Fig. 10.7). The Type field identifies the ICMP message, the Code field provides further information about the associated Type field and the Checksum field verifies the integrity of the message.

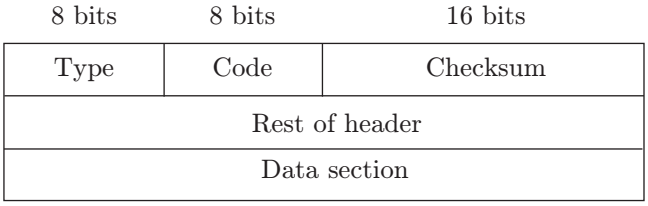


Figure 10.7 | ICMP message.

Extra options are specified in the rest of the header. ICMP places the message to be sent in the data section. Different types defined for ICMP messages are shown in Table 10.5.

Table 10.5 | Different types defined for ICMP messages

Category	Type	Message
Error Reporting Message	3	Destination Unreachable
	4	Source Quench
	11	Time Exceeded
	12	Parameter Problem
	5	Redirect Message
Query Message	0	Echo Reply
	8	Echo Request
	9	Router solicitation
	10	Router advertisement
	13	Timestamp Request
	14	Timestamp Reply
	17	Address Mask Request
	18	Address Mask Reply

10.7 LAYER 4: TRANSPORT LAYER

Although the reliability of the network layer is undoubtful, the transport layer has many responsibilities to carry out the following:

1. Managing connections and timers
2. Allowing reliable, connection-oriented byte stream from one end to other end
3. Multiplexing
4. Addressing
5. Performing segmentation
6. Packetizing
7. Handling error control and variable sized sliding window for flow control
8. Allocating bandwidth with congestion control

Issues:

(a) Headers, error detection, reliable communication
(b) Communication between processes (running on machines on possibly different networks)

10.8 CONGESTION

Congestion occurs when packets overload the subnet (means the number of packets sent to the network is greater than the capacity of the network), which results in performance degrade. The following are causes for congestion:

1. A sudden stream of packet from various sources reaching the same destination.
2. Slow links.
3. Slow processor.
4. Suppose an intermediate router has no free buffer, it will discard the packet. As the ender will not receive any acknowledgement, it will resend the packet and hence congestion will be there.

Congestion is unavoidable, but it is necessary to control it. It can be handled with the following approach:

1. Congestion information may be forwarded to the concerned node so that it is possible to limit senders (prevent one sender from overflowing the receiver) or reroute the packets.
2. Resource availability may reduce the congestion.
3. Prevent additional packets from entering the congestion region.

To control congestion in network traffic, leaky bucket algorithm is used. This algorithm shapes the bursty traffic into fixed rate traffic. It does so by averaging the data rate and dropping the packets if bucket is full.

10.8.1 Congestion Versus Flow Control

Congestion control ensures the ability to carry the offered traffic by any subnet. The major entities that effect the congestion are behaviour of hosts, routers as well as the factors that reduce the carrying capacity.

Flow control makes it sure that there is not much difference between the sending and receiving packet rate, that is, a fast sender does not send at a rate faster than the rate at which the receiver receives.

10.9 USER DATAGRAM PROTOCOL AND TRANSMISSION CONTROL PROTOCOL

10.9.1 User Datagram Protocol

UDP, or User Datagram Protocol, is an unreliable and connectionless protocol used by applications that transmit small amount of data at one time and do not require receipt of acknowledgement of data, for example, audio or video broadcasting (Fig. 10.8).

Source port (16 bits)	Destination port (16 bits)
Length (16 bits)	Checksum (16 bits)
Data	

Figure 10.8 | UDP packet.

10.9.2 Transmission Control Protocol

TCP, or Transmission Control Protocol, provides a connection-oriented, reliable stream delivery through the use of sequenced acknowledgement with retransmission of packets when necessary. The TCP header structure is shown in Fig. 10.9.

Source port (16 bits)								Destination port (16 bits)
Sequence number(32 bits)								
Acknowledgement number (32 bits)								
HLEN (4 bits)	Reserved (6 bits)	U	A	P	R	S	F	Window (16 bits)
Checksum (16 bits)								Urgent pointer (16 bits)
Option + padding								
Data								
TCP - header structure								

Figure 10.9 | TCP packet.

In TCP, sequence number is attached for every byte in the segment. The initial sequence number for the first data byte will be a random number that is generated by a random number generator in the range of 0 to $2^{32} - 1$. Acknowledgement number will always be the sequence number of the next expected data. The control bits and their description is given in Table 10.6.

Table 10.6 | Control bits

Control Bits	Description
U (URG)	Urgent pointer field significant
A (ACK)	Acknowledgement field significant
P (PSH)	Push function
R (RST)	Reset the connection
S (SYN)	Synchronize sequence numbers
F (FIN)	No more data from sender

10.10 SOCKETS

A **socket** is an endpoint for communication between client process and server process across a network. A **socket address** is the combination of an IP address and a port number. This address is used to send data packet to a particular process running on a machine. When two programs are executed, a client process and a server process are created, and these processes communicate with each other by reading from, and writing to, sockets.

There are few system calls, such as those given below:

1. Socket() returns a socket descriptor (like file descriptor), which is an integer value.
2. Bind() binds an address to a socket descriptor created by socket.
3. Listen() announces willingness to accept connections.
4. Accept() blocks the caller until a connection attempt arrives.
5. Connect() actively attempts to establish a connection.
6. Send() sends some data over the connection.
7. Receive() receives some data from the connection.
8. Close() releases the connection.

The following steps (as shown in Figure 10.10) occur when establishing a TCP connection between two computers using sockets:

1. The server instantiates a ServerSocket object, which denotes the port number on which the communication is to take place.
2. The server invokes accept() method of the ServerSocket class, which waits until a client connects to the server at the given port.
3. While the server is waiting, a client instantiates a Socket object, which specifies the server name and port number for the connection.
4. The constructor of the Socket class attempts to connect client to the specified server and port number. Once the communication is established, the client has a Socket object for communicating with the server.
5. The accept() method returns a reference to a new socket on the server that is connected to the socket of the client.

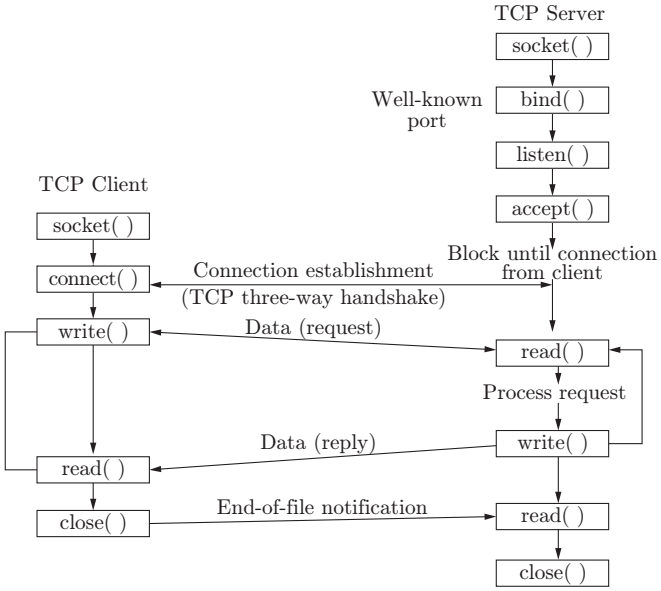


Figure 10.10 | Socket creation.

10.11 LAYER 5: SESSION LAYER

The services provided by session layer are as follows:

1. Establishes, manages and terminates a communication session with remote systems
2. Allows two machines to enter into a dialog (communication may be half duplex or full duplex)
3. Adds checkpoints or synchronisation points to a data stream.
4. Groups several user-level connections into a single 'session'.

Some protocol suites do not include the session layer.

Checkpoint: If we need a file of 1000 pages, it is suggested to insert checkpoints after every 100 pages to ensure that each 100-page unit is received and acknowledged independently. Meanwhile, if a crash occurs during the transmission of page 324, the only pages that need to be resent after system recovery are pages 301 to 324. The pages from 1 to 300 need not be resent.

10.12 LAYER 6: PRESENTATION LAYER

The following are the major concerns of presentation layer:

1. Syntax and semantics of the information exchanged between two systems.
2. Support to different encoding schemes used by different machines. It converts the sender-dependent format into a common format and the receiver converts it back to the receiver-dependent format.
3. Data encryption—to ensure privacy, sensitive information should be encrypted. Information encrypted to some other form is unreadable to others.
4. Data compression—to reduce the size of information to carry. In the case of multimedia, for example, text, audio and video, compression is a very useful tool.

Note: Many protocol suites do not include a presentation layer.

10.13 LAYER 7: APPLICATION LAYER

The major responsibility of application layer is to implement communication between two applications of the same type. There is a common misconception that every user application runs on application layer, but it runs only on those applications which interact with the communication system. For example, FTP, HTTP, SMTP/POP3/IMAP (email)are all application layer protocols, but a designing software or text editor cannot be considered as an application layer protocol.The following are popular application layer protocols:

1. **Internet Control Message Protocol (ICMP):** ICMP provides error reporting and query management mechanism for host, which lacks in IP. ICMP messages are of two types: error-reporting messages and query messages. The header of ICMP is of 8 bytes and data section is of variable size. First byte is ICMP type, second byte is code, the next two bytes specify the checksum field and rest of the header is specific for each message type.
2. **Domain Name System (DNS):** DNS is a supporting program, which is used by other programs used by the users, such as email. DNS is a client–server program used to find the IP address of an email recipient. In DNS client–server application, a sender sends an email to the email address of the receiver. The DNS client sends the request to the DNS server to map the email address to IP address. DNS has three different domains: generic, country and inverse domains. Generic domain specifies the registered hosts according to their generic behaviour. For example, com, org, edu, gov, net, etc. The country domain uses two character country abbreviations, for example, 'in' for India. The inverse domain is used to map an address to a name (Fig. 10.11).

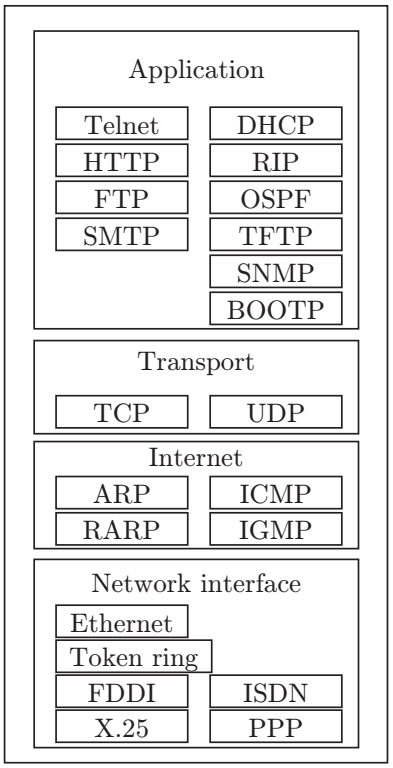


Figure 10.11 | TCP/IP protocols.

3. **Simple Mail Transfer Protocol (SMTP):** SMTP is a message transfer agent (MTA), which is used to transfer mail. A system should have client MTA for sending a mail and server MTA for receiving a mail. SMTP is used two times, between the sender and the sender's mail server and between the two mail servers. The main task of SMTP is to push the message from the client to the server.
4. **Post Office Protocol (POP):** POP3 (version 3) is a message access protocol which is used to extract the message for client to the server. It has two modes: the delete mode and the keep mode. In the delete mode, the mail is deleted from the mailbox after each retrieval, while in the keep mode, the mail remains in the mailbox after retrieval.
5. **File Transfer Protocol (FTP):** It is used for transferring files from one system to another. FTP establishes two connections between hosts, one for data transfer and the other for control information. FTP uses TCP Port 21 for the control connection

and TCP Port 20 for the data connection. The FTP client has three components: user interface, client control process and the client data transfer process. The server has two components: the server control process and the server data transfer process. The control connection remains open for entire FTP session, whereasthe data connection remains open for each file transfer.

6. **Hypertext Transfer Protocol (HTTP):** HTTP is used to access data on the World Wide Web (WWW). It works as a combination of FTP and SMTP. Unlike FTP, HTTP does not have any control connection and uses only one TCP connection. Unlike SMTP, it does not store and then forward the messages. It immediately sends the messages. HTTP uses a TCP Port 80.

10.14 DEVICES

The devices used for internetworking at different layers are specified in Fig. 10.12.

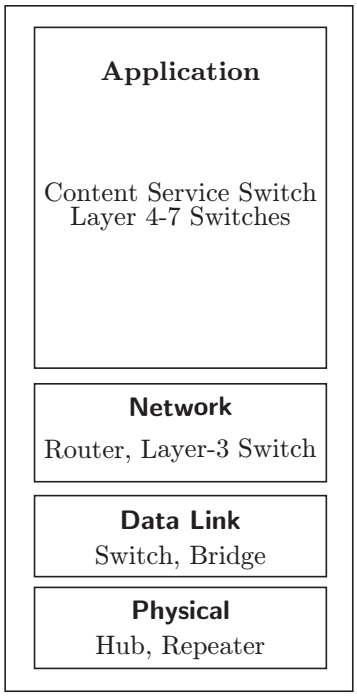


Figure 10.12 | Devices.

1. **Repeaters:** It is an electronic device which can receive the weak signal and retransmit it with higher speed. For example, if the LAN is connected for a long distance, then to cover a distance the signal is sent to a repeater which is attached with two LANs and retransmits the signal to a higher level. Thus, repeater connects two segments of network cable. It works at the physical layer of the OSI model.
2. **Bridge:** There is a limited number of stations that can be connected with a single LAN. So, a bridge is used to connect multiple LANs of the same type. It operates on a physical layer and data link layer. A bridge checks the physical address contained in the frame. It also uses table for filtering frames. It partitions the collision so that performance increases.
3. **Hub:** It is a network device which is used to connect various computers together. Hub is the central connection for all the computers, which connect through Ethernet. Hub can receive and send the information but cannot perform both tasks at the same time. This makes it slower than a switch. It is less expensive and less complex.
4. **Switch:** Switch is a small network device used to connect one or more computers through LAN. It is mostly used in home networks. Switches and hubs are used in the same network. Hubs increase the network by providing more ports, and switches divide the whole network into smaller networks. Switching reduces the amount of unnecessary traffic when every port sends the same information. Switch also reduces the possibility of collision in network.
5. **Router:** A router is a networking device which takes packets from one network and after analysis sends that packet to another network. When a data packet comes to the router, the router reads the destination address of the packet and sends it to the respective router which contains that destination address (listed in its routing table). A router is more intelligent than a hub because a hub only sends the information between the devices but the router analyses the packet and then forwards it to the other network. It controls the traffic on the network.
6. **Gateway:** It is a networking system capable of interconnecting one or more networks that has different base protocol. Gateway serves as an entry and exit point. Gateway, sometime called as protocol converter, is used in different layers. For example, a gateway can be used to convert a TCP/IP packet to a NetWare IPX packet.

Problem 10.12: If the capacity of router is 1 MB, data output rate is 8 Mbps. Tokens are generated at 6 Mbps. Calculate the time burst traffic is routed.

Solution: $C + \rho \cdot S = M \cdot S$

where M = output rate, C = capacity of router, S = time of burst traffic and ρ = token rate

$$10^6 + 6 \times 10^6 \cdot S = (8 \times 10^6) \cdot S$$
$$10^6(1 + 6S) = (8 \times 10^6) \cdot S$$
$$1 + 6S = 8S$$
$$2S = 1 \Rightarrow S = 0.5 \text{ s}$$

10.15 NETWORK SECURITY

Network security is an activity designed to protect the network and data in terms of usability, reliability, integrity and safety. It targets a variety of threats and prevents them to enter into the network. It is accomplished through hardware and software, for example, firewall, anti-virus and anti-spyware, cryptography, intrusion prevention systems (IPS) used to identify fast-spreading threats such as zero-day attacks,and virtualprivate networks (VPNs) used to provide secure remote access.

Network security components are as follows:

1. **Confidentiality:** It ensures the concealment of data to unauthorised individuals.
2. **Integrity:** It ensures that information is changed in a specified and authorised manner. There is no change in content or source by an unintended user.
3. **Availability:** It ensures that systems are available for the authorised users.

The trio form the term CIA (Confidentiality, Integrity and Availability).

10.15.1 Basic Concepts in Cryptography

Cryptography is the science of providing secure communication over insecure channels. Cryptography consists of two operations: encryption and decryption.

Encryption is the process in which data is ciphering so that only the intended recipient can know the message. Decryption is the process of deciphering the message.

Basically, encryption and decryption are two functions of a cryptographic algorithm mathematically related to each other. A cryptographic algorithm is widely known, but a key, which is used for the encryption/decryption, is kept secret.

Cryptography is of two types: symmetric cryptography and asymmetric cryptography. Both the approaches have their own pros and cons.

10.15.1.1 Symmetric Cryptography

In symmetric key cryptography, a single shared key is used for both encryption and decryption as shown in Fig. 10.13. Symmetric cryptographic primitives use block ciphers, stream ciphers, cryptographic hash functions, and message authentication codes (MACs). Block cipher uses a deterministic algorithm and operates on a block (fixed length of bits) with unaltered transformation. Stream cipher encrypts each bit individually to generate cipher text. Hash functions or one-way hash functions are used to map an arbitrary-length message string to fixed-size message string. The final value is called hash value.

Figure 10.13 Symmetric key cryptography.

The security of the symmetric key cryptography lies in the secrecy of the shared symmetric key. If the adversary captures the shared secret key, then it affects both confidentiality and authentication of the message. Examples of symmetric key cryptography are Twofish, Serpent, AES (Rijndael), Blowfish, RC4, RC5, 3DES, IDEA, SEAL, SNOW, etc.

10.15.1.2 Asymmetric Cryptography

In asymmetric cryptography, a private key is used for the decryption of a message while a public key is used for the encryption of the message as shown in Fig. 10.14. The private key needs to be kept confidential while the public key can be published freely. Asymmetric cryptography is also known as public key cryptography (PKC). PKC was introduced first by Diffie and Hellman in 1976. Public key algorithms are based on mathematical functions rather than substitution and transposition as in symmetric key cryptography. Examples of asymmetric key cryptography are Diffie-Hellman, RSA, Merkle-Hellman, Rabin, McEliece, El Gamal, Ellliptic curves, etc.

Figure 10.14 Asymmetric key cryptography.

RSA Algorithm

The RSA algorithm, developed in 1977 by Riverst, Shamir, Adelman at MIT, provides encryption and digital signatures. RSA is based on factoring of large numbers, which is not known to be NP-complete.

Encryption and decryption are as follows for a plaintext block M and cipher textblock:

$$C = M^e \bmod n$$
$$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$$

where n and e are known to both the sender and receiver, but d is only known to the receiver. Thus, the public key is $P = \{n, e\}$ and the private key $S = \{d, n\}$. It is impossible to find d given e and n.

The detailed RSA algorithm is as follows:

1. **Key generation:**
   - Choose two prime numbers p and q, keep them secret.
   - Compute $n = pq$, n is public.
   - Calculate $\phi(n) = (p-1)(q-1)$
   - Choose e with $gcd(\phi(n), e) = 1; 1 < e < \phi(n)$, which is also public.
   - Compute $d = e^{-1} \bmod \phi(n)$ and keep it private.
   - The private key consists of $S = \{d, n\}$ and public key consists of $P = \{n, e\}$.
2. **Encryption:**
   Plaintext $M < n$
   Cipher text $C = M^e \bmod n$
3. **Decryption:**
   Ciphertext C
   Plaintext $M = C^d \bmod n$

10.15.2 Digital Signature

It provides the authenticity of the origin of information to the user and verifies the information is intact. Hence, it provides authentication and data integrity. It also provides non-repudiation, which ensures that the sender cannot deny the origin of information. It is based on the public key cryptography concept.

10.15.2.1 Digital Standard Algorithm

Digital Standard Algorithm (DSA) is based on the difficulty of discrete logarithm problem (DLP). It is also based on Elgamal and Schnorr system.

DSA involves the following four steps:

1. **Key generation:**
   - *Global Public Components:* p is a prime number with 512-1024 bits, q is a prime divisor of $(p-1)$ with 160 bits, g is an integer $g = h^{(q-1)/q} \bmod p$.
   - *Users Private Key:* x is random integer less than q.
   - *Users Public Key:* $y = g^x \bmod p$
2. **Signature:**
   - For each message M, generates random k
   - Computes $r = (g^k \bmod p) \bmod q$
   - Computes $s = k^{-1}(H(M) + xr) \bmod q$
   - Signature is (r, s)
3. **Verification:**
   - Computes $w = s^{-1} \bmod q$, $u_1 = H(M)w \bmod q$
   - Computes $u_2 = rw \bmod q$, $v = (g^{u_1} y^{u_2} \bmod p) \bmod q$
   - Verify if $v = r$
4. **Correctness:**

$$\begin{aligned} v &= (g^{u_1} y^{u_2} \bmod p) \bmod q \\ &= (g^{H(M)w \bmod q} y^{rw \bmod q} \bmod p) \bmod q \\ &= (g^{H(M)w \bmod q} \boldsymbol{y}^{xrw \bmod q} \bmod p) \bmod q \\ &= (g^{(H(M)w + xrw) \bmod q} \bmod p) \bmod q \\ &= (g^{(H(M)+xr)w \bmod q} \bmod p) \bmod q \\ &= (g^{(H(M)+xr)k(H(M)+xr)^{-1} \bmod q} \bmod p) \bmod q \\ &= (g^k \bmod \boldsymbol{p}) \bmod q \\ &= r \end{aligned}$$

10.15.3 Firewall

It is a device that filters access to the protected network from the outsider network. It is an integrated collection of security measures, which are designed to prevent unauthorised electronic access to a network system. It has a predefined set of rules, which can protect private network from unauthorised access by filtering incoming or outgoing traffic. These predefined set of rules are called firewall policies.

10.15.3.1 Functions of Firewalls

1. Examining the packet header and filtering
2. Verifying the IP address or the port
3. Granting and denying access

Packets can be filtered on the basis of the following criteria:

1. Source IP address
2. Destination IP address
3. TCP/UDP source port
4. TCP/UDP destination port

10.15.3.2 Types of Firewalls

1. **Packet Filter (stateless):** It is router-based filters. It does not use any context for filtering the packets. Individual packets are accepted or rejected. It has following limitations: (i) filter rules are hard to set up, (ii) inadequate primitives, (iii) hard to manage access to RPC-based services.
2. **Stateful Filter:** It maintains records of all connections passing through it. It determines if a packet is either the start of a new connection, a part of an existing connection or is an invalid packet. It maintains tables of each active connection, including the IP addresses, ports and sequence numbers of packets.
3. **Application gateway:** It works as a proxy. It is made up of bastion hosts, which run special software to act as a proxy server. It inspects the contents of the traffic, blocking inappropriate contents, such as websites, viruses, vulnerabilities, etc.

10.15.3.3 Limitations of Firewall

1. It cannot protect against attacks that bypass the firewall.
2. It cannot protect fully against internal threats.
3. It cannot provide protection against malicious code problems such as viruses and Trojan horses, although some are capable of scanning the code.

IMPORTANT FORMULAS

Application	Protocol
SMTP	TCP
TELNET	TCP
SSH	TCP
HTTP	TCP
DNS	TCP & UDP
PING	ICMP

1. In early token release,

$$\text{Throughput for single station or } N \text{ stations} = \frac{\text{Data}}{\text{Transmission time} + (\text{Ring latency}/\text{Number of stations})}$$

2. In delayed token release,

$$\text{Throughput for single station} = \frac{\text{Data}}{\text{Transmission time} + \text{Ring latency} + (\text{Ring latency}/\text{Number of stations})}$$

$$\text{Throughput for } N \text{ stations} = \frac{\text{Data}}{\text{Ring latency} + (\text{Ring latency}/\text{Number of stations})}$$

3. $\text{Transmission time} = \dfrac{\text{Message size (bits)}}{\text{Bandwidth (bits/s)}}$

4. $\text{Propagation time} = \dfrac{\text{Distance}}{\text{Velocity}}$

5. For stop-and-wait ARQ

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

$$\text{Propagation delay} = \frac{\text{Distance of the link}}{\text{Velocity}}$$

Link utilisation of sender or throughput is given by

$$\eta = \frac{\text{Transmission time}}{\text{Transmission time} + 2 \times \text{Propagation delay}}$$

6. Pure ALOHA

$$\text{Throughput } (S) = G \times e^{-2G}$$

$$\text{Vulnerable time} = 2 \times T_{fr}$$

$$S_{\max} = 18.4\%$$

7. Slotted ALOHA

$$\text{Throughput } (S) = G \times e^{-G}$$

$$\text{Vulnerable time} = T_{fr}$$

$$S_{\max} = 36.8\%$$

SOLVED EXAMPLES

1. Which layer is responsible for delivery from process to process?

(a) Network (b) Transport
(c) Physical (d) Data link

Solution: Transport layer is responsible for end-to-end process communication.

Ans. (b)

2. The minimum size of an Ethernet frame is

(a) 18 bytes (b) 64 bytes
(c) 46 bytes (d) 56 bytes

Solution: Ethernet header = 18 Bytes [Dest. Mac (6) + Source Mac (6) + Length (2) + CRC (4)] Minimum Data Portion = 46 Bytes and Minimum Ethernet Frame Size = 64 Bytes

Ans. (b)

3. Using a 7-bit sequence number, what is the maximum size (in bits) of the sender and receiver window using stop-and-wait protocols?

(a) 1 and 1 (b) 1 and 7
(c) 7 and 1 (d) 7 and 7

Solution: Stop-and-wait protocol uses 1 bit sequence.

Ans. (a)

4. Vulnerable time in CSMA is

(a) It is double the transmission time as it includes the sensing time
(b) Half of average frame transmission time as collisions are less
(c) $2 \times$ (the average frame transmission time)
(d) None of the above

Solution: Vulnerable time for CSMA is the propagation time T_p needed for a signal to propagate from one end of the medium to the other.

Ans. (d)

5. Which class of IP addresses is used for multicasting?

(a) Class E (b) Class C
(c) Class A (d) Class D

Solution: Class D is used for multicasting. Refer Table 10.4.

Ans. (a)

6. The options field of IPv4 is used for?

(a) Time stamping, strict source routing
(b) Loose source routing, strict source routing
(c) Time stamping only
(d) Time stamping, loose source routing, strict source routing

Solution: It may contain values for various options, such as strict source routing, security, record route, time stamp, etc.

Ans. (d)

7. In a fully connected mesh network with d devices and c connections, there are _____ physical channels to link all devices.

(a) $d^*(d-1)/2$ (b) $d^*(d+1)/2^*c$
(c) $(2^*d + 2^*c)/2$ (d) $2^*(d+1)+c$

Solution: The total number of wired links required to establish a fully connected mesh network of d nodes can be calculated as $c = d\,(d-1)/2$.

Ans. (a)

8. In IPv4 header, the _____ field is used to determine to which datagram a newly arrived fragment belongs to.

(a) Identification (b) Datagram_id
(c) Fragment offset (d) Time to live

Solution: Identification field is used to identify original IP packet the fragments belong to.

Ans. (a)

9. Encryption and decryption is the responsibility of _____ layer.

(a) Session (b) Data link
(c) Application (d) Network

Solution: Application layer is responsible for the encryption and decryption processes.

Ans. (c)

10. Maximum throughput of an ALOHA network is

(a) 18.4% (b) 35.8% (c) 36.8% (d) 50%

Solution: When $G = 1$, the throughput is increased to the maximum value of 36.8%.

Ans. (c)

11. A terminal multiplexer has six 1200 bps terminals and 'N' 300 bps terminals connected to it. The outgoing line is 9600 bps. What is the maximum value of N?

(a) 4 (b) 6 (c) 8 (d) 12

Solution: Since, there are six 1200 bps terminals. So, $6 \times 1200 + n \times 300 = 9600 \Rightarrow n = 8$

Ans. (c)

12. The total number of wired links required to establish a fully connected mesh network of 9 nodes will be

(a) 36 (b) 56 (c) 72 (d) 64

Solution: Total number of wired links required to establish a fully connected mesh network of n nodes can be calculated as $c = n(n-1)/2$
So, for 9 nodes, total links are 36.

Ans. (a)

13. Considering a classful addressing, the IP address 128.252.144.84 denotes

(a) 0.0.0.0 as network ID and 128.252.252.84 as node ID
(b) 128.0.0.0 as network ID and 128.252.127.84 as node ID
(c) 128.252.0.0 as network ID and 128.252.144.84 as node ID
(d) 128.252.144.0 as network ID and 128.252.144.84 as node ID

Solution: The IP belongs to class B. The network id is 128.252.0.0 and the node id is 128.252.144.84.

Ans. (c)

14. In Ethernet CSMA/CD, the special bit sequence transmitted by media access management for collision handling is called

(a) Hamming code (b) CRC
(c) Jam (d) Preamble

Solution: Hamming code is a set of error-correction code, which is used to detect and correct bit errors. CRC (cyclic redundancy check) is used to detect data transmission errors.
Preamble is used in network communications for synchronizing transmission time between systems.

Ans. (c)

15. A Gateway operates at _____ layers.

(a) All layers except physical and application layer
(b) All the seven layers
(c) Only on session, transport and network layers
(d) Same layers on which the switch and bridge operates

Solution: Hubs, repeaters(or active hubs) operate at physical layer (1); Bridges, Switches operates at data link layer (2) ; Routers operate at network layer (3) ; content-switches (or web-switches or application-switches) operates at layers 4 to 7. Gateway operates at all the seven layers–physical, data link, network, transport (4), session (5), presentation (6), application (7).

Ans. (b)

16. Consider the network with subnet mask 153.224.0.0/13. Determine the last host address in the network.

(a) 153.208.255.255
(b) 153.224.255.254
(c) 153.231.255.255
(d) 153.231.255.254

Solution: Network id: 153.224.0.0
Subnet mask: 255.248.0.0
By doing XOR between network id and subnet mask, one gets network id= 153.231.0.0
We have 19 bits for host, so first host address is 153.224.0.1 and last host is 153.231.255.254

Ans. (d)

17. Consider a token ring LAN of length 12 km and having 40 stations, signal propagation speed is 8 ns/m and data rate is 100 Mbps. An average frame contains 220 bytes. Delay occurred at each station is equivalent to 10-bit delay. What is the utilisation of token ring approximately?

(a) 10% (b) 12%
(c) 15% (d) 21%

Solution: Transmission time of a frame

$$T_t = \frac{220 \times 8}{100 \times 10^6} \text{ s} = 17.6 \ \mu\text{s}$$

Propagation time around the ring

$$T_p = 10 \times 12000 \text{ ns} = 120 \ \mu\text{s}$$

Delay at each station = 1/10 μs, so delay at 40 stations will be = 4 μs
Now,

$$\text{Utilisation (U)} = \frac{T_t}{T_t + T_p + \text{delay at all stations}}$$
$$= \frac{17.6}{17.6 + 120 + 4} = \frac{17.6}{141.6}$$
$$= 0.124 \times 100 = 12.4\% \approx 12\%$$

Ans. (b)

18. A CSMA/CD-based network has transmission rate 120 Mbps, length 1 km and speed of signal is 10^9 m/s. What should be the minimum frame size?

(a) 120 B (b) 240 B
(c) 400 B (d) 440 B

Solution: We know that

$$\frac{\text{Length of packet}}{\text{Bandwidth}} = 2 \times \frac{\text{Distance}}{\text{Velocity}}$$

$$\text{So, packet length} = 2 \times \frac{1000}{10^9} \times 120 \times 10^6 \Rightarrow 240 \text{ bytes}$$

Ans. (b)

19. How many 8-bit characters can be transmitted per second over a 7800 baud serial communication link using asynchronous mode of transmission with one start bit, 8 data bits and 1 parity bit?

(a) 600 (b) 660
(c) 780 (d) 1200

Solution: Total number of bits = 10

Modulation rate = 7800 baud

Numbers of 8-bit characters are transmitted = $\frac{7800}{10 \text{ bits}} = 780$

Ans. (c)

20. In a token ring network, the transmission speed is 20 bps and the propagation speed is 180 m/μs. The 1-bit delay in this network is equivalent to:

(a) 20 m of cable (b) 18 m of cable
(c) 9 m of cable (d) 5 m of cable

Solution: Given that $R = 2\times10^7$ bps, $B = 1$ bps, $V = 180$ m/μs; d =?

$$B = R \times \frac{d}{v}$$

$$d = \frac{Bv}{R} = \frac{1\times180}{2\times10^7 \times10^{-6}} = 9 \text{ m of cable}$$

Ans. (c)

21. Determine the maximum length of the cable (in km) for transmitting data at a rate of 400 Mbps in an Ethernet LAN with frames of size 8000 bits. Assume the signal speed in the cable to be 250000 km/s.

(a) 4 b) 5 (c) 5.5 (d) 7

Solution: Maximum length of cable can be calculated by the given problem:

$$\frac{8000 \text{ bits}}{400\times10^6 \text{ bits/s}} = \frac{2\times L}{25\times10^4 \text{km/s}}$$

$$L = 5 \text{ km}$$

Ans. (b)

22. In the IPv4 addressing format, the number of networks allowed in class C addresses is

(a) 2^{21} (b) 2^{22}
(c) 2^{23} (d) 2^{24}

Solution: In class C,
Net id = 24 bit
Host id = 8 bits
Out of 24 bits 3 bits are reserved for representation class 'C', that is, 110.
So, C class has 2^{21}networks.

Ans. (a)

23. Consider a 2.5 Mbps token ring LAN and frame size of 180 bytes. If the ring latency is 210 μs, then what will be the effective data rate of the LAN?

(a) 1.40 Mbps (b) 1.56 Mbps
(c) 1.76 Mbps (d) 1.84 Mbps

Solution:

$$\text{Transmission time} = \frac{\text{Data size}}{\text{Bandwidth}} = \frac{180\times8}{2.5\times10^6} = 0.00057 \text{ s}$$

Ring latency = Round-trip time = 210 μs = 0.00021 s
Total time required to transfer 1440 bits = (0.00057 + 0.00021) = 0.00078 s
So, effective data rate = 1440/0.00078 = 1.84 Mbps

Ans. (d)

24. How many number of parity bit is required in hamming code if message size is 8 bit?

(a) 2 (b) 4
(c) 6 (d) 8

Solution:
Given message (m) = 8-bit
To calculate the number of parity bits, we have the formula:

$2^r \geq m + r + 1$, by putting $r = 1, 2, 3, 4\ldots$
$r = 4$ will satisfy the given equality.

Ans. (b)

GATE PREVIOUS YEARS' QUESTIONS

1. Which of the following assertions is FALSE about the Internet Protocol (IP)?

(a) It is possible for a computer to have multiple IP addresses.
(b) IP packets from the same source to the same destination can take different routes in the network.
(c) IP ensures that a packet is discarded if it is unable to reach its destination within a given number of hops.
(d) The packet source cannot set the route of an outgoing packet; the route is determined only by the routing tables in the routers on the way.

(GATE 2003: 1 Mark)

Solution: The packet source can set the route of an outgoing packet; the route is determined only by the routing tables in the routers on the way.

Ans. (d)

2. Which of the following functionalities must be implemented by a transport protocol over and above the network protocol?

(a) Recovery from packet losses
(b) Detection of duplicate packets
(c) Packet delivery in the correct order
(d) End-to-end connectivity

(GATE 2003: 1 Mark)

Solution: End-to-end delivery is the responsibility of a transport layer.

Ans. (d)

3. The subnet mask for a particular network is 255.255.31.0. Which of the following pairs of IP addresses could belong to this network?

(a) 172.57.88.62 and 172.56.87.233
(b) 10.35.28.2 and 10.35.29.4
(c) 191.203.31.87 and 191.234.31.88
(d) 128.8.129.43 and 128.8.161.55

(GATE 2003: 2 Marks)

Solution: The two addresses should belong to the same network, if binary AND operation of both addresses with net mask should be same.

The last octets of IP addresses of 0 is 000 0000.
The last octets of IP address of 43 and 55 and their AND with net mask gives the same result.

Ans. (d)

4. A 2-km long broadcast LAN has 10^7 bps bandwidth and uses CSMA/CD. The signal travels along the wire at 2×10^8 m/s. What is the minimum packet size that can be used on this network?

(a) 50 bytes (b) 100 bytes
(c) 200 bytes (d) None of the above

(GATE 2003: 2 Marks)

Solution: Given that length $L = 2$ km $= 2000$ m

Bandwidth, $B = 10^7$ bps
Signal travels $S = 2 \times 10^8$ m/s

So, propagation delay $(T_p) = \dfrac{L}{S} = \dfrac{2\times10^3}{2\times10^8} = \dfrac{1}{10^5}$ s

In CSMA/CD network,

Round-trip delay $= 2 \times T_p = 2 \times 10^5$ s
The minimum packet size must take round-trip delay to transmit.
So, transmission delay (T_x) = Round-trip delay

Since $T_x = N/B$, where N is the number of bits to be transmitted.
Number of bits transmitted, N = Round-trip delay $\times B = 2 \times 10^5 \times 10^7 = 200$ bytes

Ans. (c)

5. Host A is sending data to host B over a full duplex link. A and B are using the sliding window protocol for flow control. The send and receive window sizes are 5 packets each. Data packets (sent only from A to B) are all 1000 bytes long and the transmission time for such a packet is 50 μs. Acknowledgement packets (sent only from B to A) are very small and require negligible transmission time. The propagation delay over the link is 200 μs. What is the maximum achievable throughput in this communication?

(a) 7.69×10^6 bps (b) 11.11×10^6 bps
(c) 12.33×10^6 bps (d) 15.00×10^6 bps

(GATE 2003: 2 Marks)

Solution:
Throughput = 1 window/RTT
Round-trip time (RTT) = Transmission time + 2 × Propagation time

$$= 50 \text{ ms} + 2 \times 200 \text{ ms} = 450 \text{ ms}$$

As the size of window is 5 packets and 1 packet contains 1000 bytes.
The total size of the packet in bytes is $5 \times 1000 = 50000$ bytes

$$\text{Therefore, throughput} = \frac{5000 \text{ bytes}}{450\times10^{-6} \text{ s}}$$

$$= 11.11\times10^6 \text{ bps}$$

Ans. (b)

6. Choose the best matching between Groups 1 and 2.

Group: 1	Group: 2
P. Data link layer	1. Ensures reliable transport of data over a physical point-to-point link
Q. Network layer	2. Encodes/decodes data for physical transmission
R. Transport layer	3. Allows end-to-end communication between two processes
	4. Routes data from one network node to the next

(a) P:1, Q:4, R:3 (b) P:2, Q:4, R:1
(c) P:2, Q:3, R:1 (d) P:1, Q:3, R:2

(GATE 2004: 1 Mark)

Solution: Data link layer provides reliable transmission of data over a physical link.
Network layer provides routing of data packets in the network.
Transport layer is responsible for end-to-end process communication.

Ans. (a)

7. Which of the following is NOT true with respect to a transparent bridge and a router?

(a) Both bridge and router selectively forward data packets.
(b) A bridge uses IP addresses while a router uses MAC addresses.
(c) A bridge builds up its routing table by inspecting incoming packets.
(d) A router can connect between a LAN and a WAN.

(GATE 2004: 1 Mark)

Solution: Both router and bridge selectively forward data packets and both can connect between a LAN and WAN. Routing and bridge builds their routing table by inspecting incoming packets but router and bridge both use MAC address. So, option (b) is correct.

Ans. (b)

8. How many 8-bit characters can be transmitted per second over a 9600 baudserial communication link using asynchronous mode of transmission with one start bit, eight data bits, two stop bits, and one parity bit?

(GATE 2004: 1 Mark)

(a) 600 (b) 800 (c) 876 (d) 1200

Solution:

$$\frac{9600}{1+8+2+1} = 800$$

Ans. (b)

9. A and B are the only two stations on an Ethernet. Each has a steady queue of frames to send. Both A and B attempt to transmit a frame, collide, and A wins the first back-off race. At the end of this successful transmission by A, both A and B attempt to transmit and collide. The probability that A wins the second back-off race is

(a) 0.5 (b) 0.625 (c) 0.75 (d) 1.0

(GATE 2004: 2 Marks)

Solution: At the first collision, both A and B will have first collision but A wins.
So, A's collision counter will be reinitialized to 0.
At the second collision, A and B will have first and second collisions, respectively.
So, A will have to select random number from [0,1].
But, B will have to select from [0, 1, 2, 3].
On mapping, the following are total favouring cases to A's winning.

0–1 0–2 0–3 1–2 1–3

So, the probability is $5/8 = 0.625$.

Ans. (b)

10. The routing table of a router is shown below:

Destination	Subnet Mask	Interface
128.75.43.0	255.255.255.0	Eth_0
128.75.43.0	255.255.255.128	Eth_1
192.12.17.5	255.255.255.255	Eth_3
Default		Eth_2

On which interface will the router forward packets addressed to destinations 128.75.43.16 and 192.12.17.10, respectively?

(a) Eth_1 and Eth_2 (b) Eth_0 and Eth_2
(c) Eth_0 and Eth_3 (d) Eth_1 and Eth_3

(GATE 2004: 2 Marks)

Solution: On performing AND operation between incoming IP address and subnet-mask and comparing the result with the destination.

If there is a match between multiple destinations, then select the destination with the longest length subnet mask.

128.75.43.16 matches with 128.75.43.0 and 128.75.43.0. But the packets addressed to 128.75.43.16 will be forwarded to Eth_1.

If a result is not matching with any of the given destinations, then the packet is forwarded to the default interface (here Eth_2).

Therefore, the packets addressed to 192.12.17.10 will be forwarded to Eth_2.

Ans. (a)

Common Data Questions 11 and 12: Consider three IP networks A, B and C. Host H_A in network A sends messages each containing 180 bytes of application data to a host H_C in network C. The TCP layer prefixes a 20-byte header to the message. This passes through an intermediate network B. The maximum packet size, including 20-byte IP header, in each network is

A: 1000 bytes
B: 100 bytes
C: 1000 bytes

The network A and B are connected through a 1 Mbps link, while B and C are connected by a 512 Kbps link (bps = bits per second).

11. Assuming that the packets are correctly delivered, how many bytes, including headers, are delivered to the IP layer at the destination for one application message, in the best case? Consider only data packets.

(a) 200 (b) 220
(c) 240 (d) 260

(GATE 2004: 2 Marks)

Solution: When all the 3 packets are delivered, the bytes are

$$(80 + 20) + (80 + 20) + (40 + 20) = 260$$

Ans. (d)

12. What is the rate at which application data is transferred to host H_C? Ignore errors, acknowledgements and other overheads.

(a) 325.5 Kbps (b) 354.5 Kbps
(c) 409.6 Kbps (d) 512.0 Kbps

(GATE 2004: 2 Marks)

Solution: Actual data sent =180 out of 260
So, data rate $(180/260) \times 512$ Kbps = 354.461 Kbps

Ans. (b)

13. Packets of the same session may be routed through different paths in:

(a) TCP, but not UDP (b) TCP and UDP
(c) UDP, but not TCP (d) Neither TCP nor UDP

(GATE 2005: 1 Mark)

Solution: Packets travel on network layer. TCP and UDP are transport layer protocols.

Ans. (b)

14. The address resolution protocol (ARP) is used for:

(a) finding the IP address from the DNS.
(b) finding the IP address of the default gateway.
(c) finding the IP address that corresponds to a MAC address.
(d) finding the MAC address that corresponds to an IP address.

(GATE 2005: 1 Mark)

Solution: ARP works to find the physical address of a machine.

Ans. (d)

15. The maximum window size for data transmission using the selective reject protocol with n-bit frame sequence numbers is

(a) 2^n (b) 2^{n-1} (c) $2^n - 1$ (d) 2^{n-2}

(GATE 2005: 1 Mark)

Solution: For selective reject protocol, window size $= 2^n/2 = 2^{n-1}$

Ans. (b)

16. In a network of LANs connected by bridges, packets are sent from one LAN to another through intermediate bridges. Since more than one path may exist between two LANs, packets may have to be routed through multiple bridges. Why is the spanning tree algorithm used for bridgerouting?

(a) For shortest path routing between LANs
(b) For avoiding loops in the routing paths
(c) For fault tolerance
(d) For minimising collisions

(GATE 2005: 1 Mark)

Solution: Spanning tree protocol is used for bridge routing to avoid loops in routing paths.

Ans. (b)

17. An organisation has a class B network and wishes to form subnets for 64 departments. The subnet mask would be

(a) 255.255.0.0 (b) 255.255.64.0
(c) 255.255.128.0 (d) 255.255.252.0

(GATE 2005: 1 Mark)

Solution: For class B, 16 bits are reserved as network bits. To allocate 64 subnets, 6 bits are added to network bits. 22 bits are for network. Subnet mask is created by assigning 1 to all network bits.
So, mask is 255.255.252.0.

Ans. (d)

18. In a packet-switching network, packets are routed from source to destination along a single path having two intermediate nodes. If the message size is 24 bytes and each packet contains a header of 3 bytes, then the optimum packet size is

(a) 4 (b) 6 (c) 7 (d) 9

(GATE 2005: 2 Marks)

Solution: Optimal packet size is 9.

9−3 = 6 B will be transferred in one packet, so the total message will travel in 4 packets.

Ans. (d)

19. Suppose the round-trip propagation delay for a 10 Mbps Ethernet having 48-bit jamming signal is 46.4 s. The minimum frame size is

(a) 94 (b) 416
(c) 464 (d) 512

(GATE 2005: 2 Marks)

Solution: RTT = 46.4×10^{-6}s

10 Mb are sent in = 1 s
1 will be sent = $1/10^7$
48 bits will be in = 4.8×10^{-6} s
Total delay = 46.4 + 4.8 = 51.2
Minimum frame size = $51.2 \times 10 = 512$ bits

Ans. (d)

20. For which one of the following reasons does Internet Protocol (IP) use the time- to-live (TTL) field in the IP datagram header?

(a) Ensure packets reach destination within that time
(b) Discard packets that reach later than that time
(c) Prevent packets from looping indefinitely
(d) Limit the time for which a packet gets queued in intermediate routers

(GATE 2006: 1 Mark)

Solution: Decrementing TTL will prevent packet from looping.

Ans. (b)

21. Station A uses 32 byte packets to transmit messages to Station B using a sliding window protocol. The round trip delay between A and B is 80 milliseconds and the bottleneck bandwidth on the path between A and B is 128 kbps. What is the optimal window size that A should use?

(a) 20 (b) 40
(c) 160 (d) 320

(GATE 2006: 2 Marks)

Solution: Round-trip delay = 80 ms

Bandwidth = 128 Kbps
In 1 s = 128 Kbits are sent
In 80 ms = $128\text{K} \times 80 \times 10^{-3} = 128 \times 80$ bits

$$\text{Window size} = \frac{128 \times 80}{32 \times 8} = 40$$

Ans. (b)

22. Two computers C_1 and C_2 are configured as follows. C_1 has IP address 203.197.2.53 and netmask 255.255.128.0. C_2 has IP address 203.197.75.201 and netmask 255.255.192.0. Which one of the following statements is true?

(a) C_1 and C_2 both assume they are on the same network.
(b) C_2 assumes C_1 is on the same network, but C_1 assumes C_2 is on a different network.
(c) C_1 assumes C_2 is on the same network, but C_2 assumes C_1 is on a different network.
(d) C_1 and C_2 both assume they are on different networks.

(GATE 2006: 2 Marks)

Solution: Network address of C_1: 203.197.2.53 AND 255.255.128.0 = 203.197.0.0

Network address of C_2: 203.197.75.201 AND 255.255.192.0 = 203.197.0.0
C_1 assumes C_2 is on the same network, but C_2 assumes C_1 on different network.

Ans. (c)

23. Station A needs to send a message consisting of 9 packets to station B using a sliding window (window size 3) and Go-Back-N error control strategy. All packets are ready and immediately available for transmission. If every 5thpacket that A transmits gets lost (but no packets from B ever get lost), then what is the number of packets that A will transmit for sending the message to B?

(a) 12 (b) 14 (c) 16 (d) 18

(GATE 2006: 2 Marks)

Solution:

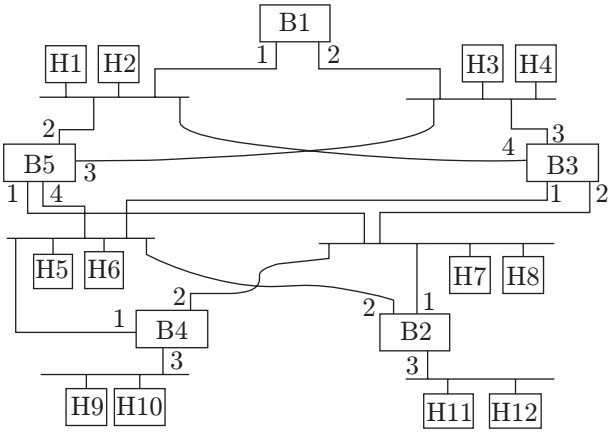
A		B
1	→	1
2	→	2
3	→	3
4	→	4
5	→	lost
6	→	discard
7	→	discard
8	→	5
9	→	6
10	→	lost 7
11	→	discard 8
12	→	discard 9
13	→	7
14	→	8
15	→	lost 9
16	→	9

Ans. (c)

Linked Answer Questions 24 and 25: Consider the diagram shown below where a number of LANs

are connected by (transparent) bridges. To avoid packets looping through circuits in the graph, the bridges organize themselves in a spanning tree. First, the root bridge is identified as the bridge with the least serial number. Next, the root sends out (one or more) data units to enable the setting up of the spanning tree of shortest paths from the root bridge to each bridge.

Each bridge identifies a port (the root port) through which it will forward frames to the root bridge. Port conflicts are always resolved in favour of the port with the lower index value. When there is a possibility of multiple bridges forwarding to the same LAN (but not through the root port), ties are broken as follows: bridges closest to the root get preference and between such bridges the one with the lowest serial number is preferred.



24. For the given connection of LANs by bridges, which one of the following choices represents the depth first traversal of the spanning tree of bridges?

(a) B_1, B_5, B_3, B_4, B_2 (b) B_1, B_3, B_5, B_2, B_4
(c) B_1, B_5, B_2, B_3, B_4 (d) B_1, B_3, B_4, B_5, B_2

Solution: DFS (depth first search) is analgorithm for traversing tree or graph. One starts at the root (selecting some arbitrary node as the root in the case of a graph) and explores as far as possible along each branch before backtracking. So depth first search traversal is B_1, B_5, B_3, B_4, B_2.

(GATE 2006: 2 Marks)

Ans. (a)

25. Consider the correct spanning tree for the previous question. Let host H_1 send out a broadcast ping packet. Which of the following options represents the correct forwarding table on B_3?

(a)

Hosts	Port
H_1, H_2, H_3, H_4	3
H_5, H_6, H_9, H_{10}	1
H_7, H_8, H_{11}, H_{12}	2

(b)

Hosts	Port
H_1, H_2	4
H_3, H_4	3
H_5, H_6	1
H_5, H_8, H_9, H_{10}, H_{11}, H_{12}	2

(c)

Hosts	Port
H_3, H_4	3
H_5, H_6, H_9, H_{10}	1
H_1, H_2	4
H_7, H_8, H_{11}, H_{12}	2

(d)

Hosts	Port
H_1, H_2, H_3, H_4	3
H_5, H_7, H_9, H_{10}	1
H_7, H_8, H_{11}, H_{12}	4

(GATE 2006: 2 Marks)

Solution: Forwarding table for B_3 is

Hosts	Port
H_1, H_2, H_3, H_4	3
H_5, H_6, H_9, H_{10}	1
H_7, H_8, H_{11}, H_{12}	2

Ans. (a)

26. In Ethernet, when Manchester encoding is used, the bit rate is

(a) Half the baud rate (b) Twice the baud rate
(c) Same as the baud rate (d) None of the above

(GATE 2007: 1 Mark)

Solution: For transmission of digital information, Manchester coding is used to convert digital information into electrical signals for transmission. It uses two baud for one bit.

Ans. (b)

27. Which one of the following uses UDP as the transport protocol?

(a) HTTP (b) Telnet
(c) DNS (d) SMTP

(GATE 2007: 1 Mark)

Solution: DNS uses services of UDP protocol.

Ans. (c)

28. There are n stations in a slotted LAN. Each station attempts to transmit with a probability p in each time slot. What is the probability that ONLY one station transmits in a given time slot?

(a) $np(p\ 1)^{n-1}$ (b) $(1-p)^{n-1}$
(c) $p(p\ 1)^{n-1}$ (d) $1-(p\ 1)^{n-1}$

(GATE 2007: 2 Marks)

Solution: Probability of sending by one station = $p(1-p)^{n-1}$

For n stations, it is $np(1-p)^{n-1}$

Ans. (a)

29. In a token ring network, the transmission speed is 10^7 bps and the propagation speed is 200 m/μs. The 1-bit delay in this network is equivalent to:

(a) 500 m of cable (b) 200 m of cable
(c) 20 m of cable (d) 50 m of cable

(GATE 2007: 2 Marks)

Solution: Transmission delay for 1 bit $t = 1/(10^7)$ = 0.1 μs.

200 m can be travelled in 1 μs. Therefore, in 0.1 μs, 20 m can be travelled.

Ans. (c)

30. The address of a class B host is to be split into subnets with a 6-bit subnet number. What is the maximum number of subnets and the maximum number of hosts in each subnet?

(a) 62 subnets and 262142 hosts
(b) 64 subnets and 262142 hosts
(c) 62 subnets and 1022 hosts
(d) 64 subnets and 1024 hosts

(GATE 2007: 2 Marks)

Solution: Here 16 + 6 = 22 bits are reserved for the network

Number of hosts = $2^{32-22} = 2^{10} - 2 = 1022$
Number of subnets = $2^6 - 2 = 62$

Ans. (c)

31. The message 11001001 is to be transmitted using the CRC polynomial $x^3 + 1$ to protect it from errors. The message that should be transmitted is

(a) 11001001000 (b) 11001001011
(c) 11001010 (d) 110010010011

(GATE 2007: 2 Marks)

Solution: The polynomial is equivalent to 1001. Divide 1001 with 11001001000 and find the remainder. Remainder is 011. Append 011 at the end of input string, it will be 11001001011.

Ans. (b)

32. The distance between two stations M and N is L km. All frames are K bits long. The propagation delay per kilometre is t s. Let R bits/s be the channel capacity. Assuming that processing delay is negligible, the minimum number of bits for the sequence number field in a frame for maximum utilisation, when the sliding window protocol is used, is

(a) $\left\lceil \log_2 \frac{2LtR+2K}{K} \right\rceil$ (b) $\left\lceil \log_2 \frac{2LtR}{K} \right\rceil$
(c) $\left\lceil \log_2 \frac{2LtR+K}{K} \right\rceil$ (d) $\left\lceil \log_2 \frac{2LtR+K}{2K} \right\rceil$

(GATE 2007: 2 Marks)

Solution: Distance between stations M and N = L km
Propagation delay = t s
Total propagation delay = Lt s
Frame size = K bits
Channel capacity = R bits/s
Transmission time = K/R
Let n be the window size.

$$\text{Utilisation} = \frac{n}{1+2a}, \text{ where } a = \frac{\text{Propagation time}}{\text{Transmission}}$$

$$= \frac{n}{1+(2LtR\ /\ K)} = \frac{nK}{2LtR+K}$$

For maximum utilisation: $nK = 2LtR + K$

Therefore, $$n = \frac{2LtR+K}{K}$$

Number of bits needed for n frames is log n.

Ans. (c)

33. Match the following:

Column I	Column II
(P) SMTP	(1) Application layer
(Q) BGP	(2) Transport layer
(R) TCP	(3) Data link layer
(S) PPP	(4) Network layer
	(5) Physical layer

(a) P − 2, Q − 1, R − 3, S − 5
(b) P − 1, Q − 4, R − 2, S − 3
(c) P − 1, Q − 4, R − 2, S − 5
(d) P − 2, Q − 4, R − 1, S − 3

(GATE 2007: 2 Marks)

Solution:
SMTP: Application layer for mail transfer
BGP: Network layer routing protocol
TCP: Transport layer transmission protocol
PPP: Data link layer protocol for direct connections

Ans. (b)

34. What is the maximum size of data that the application layer can pass on to the TCP layer below?

(A) Any size
(B) 2^{16} bytes − size of TCP header
(C) 2^{16} bytes
(D) 1500 bytes

(GATE 2008: 1 Mark)

Solution:
There is no limit of data passing at application layer.

Ans. (a)

35. Which of the following system calls results in the sending of SYN packets?

(a) Socket (b) Bind
(c) Listen (d) Connect

(GATE 2008: 1 Mark)

Solution: Connect() is called by the client and connection is established using three-way hand shake.

Ans. (d)

36. In the slow start phase of the TCP congestion control algorithm, the size of the congestion window

(a) does not increase.
(b) increases linearly.
(c) increase quadratically.
(d) increase exponentially.

(GATE 2008: 2 Marks)

Solution: In the slow start phase of the TCP congestion control algorithm, the size of the congestion window increases exponentially.

Ans. (d)

37. If a class B network on the Internet has a subnet mask of 255.255.248.0, what is the maximum number of hosts per subnet?

(a) 1022 (b) 1023
(c) 2046 (d) 2047

(GATE 2008: 2 Marks)

Solution: Number of network bits = 21

Number of host bits = 11
Number of hosts = $2^{11} - 2 = 2046$

Ans. (c)

38. A computer on a 10 Mbps network is regulated by a token bucket. The token bucket is filled at a rate of 2 Mbps. It is initially filled to capacity with 16 Mbits.

What is the maximum duration for which the computer can transmit at the full 10 Mbps?

(a) 1.6 s (b) 2 s
(c) 5 s (d) 8 s

(GATE 2008: 2 Marks)

Solution: Data transfer of token bucket = 10 Mbps
Rate of transfer = 2 Mbps

Initially filled capacity = 16 Mbits

$$\text{Maximum burst time} = \frac{b}{M-r} = \frac{16}{10-2} = 2 \text{ s}$$

Ans. (b)

39. A client process P needs to make a TCP connection to a server process S. Consider the following situation: the server process S executes a socket(), a bind() and a listen() system call in that order, following which it is pre-empted.

Subsequently, the client process P executes a socket() system call followed by connect() system call to connect to the server process S. The server process has not executed any accept() system call. Which one of the following events could take place?

(a) Connect() system call returns successfully
(b) Connect() system call blocks
(c) Connect() system call returns an error
(d) Connect() system call results in a core dump

(GATE 2008: 2 Marks)

Solution: The accept() call does not execute. So, connect() call did not get response for a time stamp to wait, therefore, connect() system call returns an error.

Ans. (c)

40. In the RSA public key cryptosystem, the private and public keys are (e,n) and (d,n), respectively, where $n = p^*q$ and p and q are large primes. Besides, n is public and p and q are private. Let M be an integer such that $0 < M < n$ and $\phi(n) = (p-1)(q-1)$. Now, consider the following equations:

I. $M' = M^e \bmod n$
$M = (M')^d \bmod n$
II. $ed \equiv 1 \bmod n$
III. $ed \equiv 1 \bmod \phi(n)$
IV. $M' = M^e \bmod \phi(n)$
$M = (M')^d \bmod \phi(n)$

Which of the above equations correctly represent the RSA cryptosystem?

(a) I and II (b) I and III
(c) II and IV (d) III and IV

(GATE 2009: 2 Marks)

Solution: Encryption: $M' = M^e \bmod n$
Decryption: $M = (M')^d \bmod n$
$ed \equiv 1 \bmod f(n)$

Ans. (b)

41. While opening a TCP connection, the initial sequence number is to be derived using a time-of-day (ToD) clock that keeps running even when the host is down. The low order 32 bits of the counter of the ToD clock is to be used for the initial sequence numbers. The clock counter increments once per millisecond. The maximum packet lifetime is given to be 64s.

Which one of the choices given below is closest to the minimum permissible rate at which sequence numbers used for packets of a connection can increase?

(a) 0.015/s (b) 0.064/s
(c) 0.135/s (d) 0.327/s

(GATE 2009: 2 Marks)

Solution: The frames from the sending station are numbered sequentially.

Ans. (b)

42. Let $G(x)$ be the generator polynomial used for CRC checking. What is the condition that should be satisfied by $G(x)$ to detect odd number of bits in error?

(a) $G(x)$ contains more than two terms.
(b) $G(x)$ does not divide $1+x^k$, for any not exceeding the frame length k.
(c) $1+x$ is a factor of $G(x)$.
(d) $G(x)$ has an odd number of terms.

(GATE 2009: 2 Marks)

Solution: To detect odd number of errors, $(x + 1)$ must be present.

Ans. (c)

Linked Answer Questions 43 and 44: Frames of 1000 bits are sent over a 10 bps duplex link between two hosts. The 6 propagation time is 25 ms. Frames are to be transmitted into this link to maximally pack them in transit (within the link).

43. What is the minimum number of bits (l) that will be required to represent the sequence numbers distinctly? Assume that no time gap needs to be given between transmissions of two frames.

(a) $l = 2$ (b) $l = 3$
(c) $l = 4$ (d) $l = 5$

(GATE 2009: 2 Marks)

Solution: Transmission delay of link = $1000/10^6$ = 1 ms

Propagation delay = 25 ms
Maximum 25 frames can be sent, for 25 frames bits required are 5.

Ans. (d)

44. Suppose that the sliding window protocol is used with the sender window size of 2^l, where l is the number of bits identified in the earlier part and l acknowledgements are always piggy backed. After sending 2^l frames, what is the minimum time the sender will have to wait before starting transmission of the next frame? (Identify the closest choice ignoring the frame processing time.)

(a) 16 ms (b) 18 ms (c) 20 ms (d) 22 ms

(GATE 2009: 2 Marks)

Solution: Size of window = 32

Round trip time = 2 × 25 ms = 50 ms
To send the next frame, the sender has to wait for 50 − 32 = 18 ms

Ans. (b)

45. One of the header fields in an IP datagram is the time-to-live (TTL) field. Which of the following statements best explains the need for this field?

(a) It can be used to prioritise packets.
(b) It can be used to reduce delays.
(c) It can be used to optimise throughput.
(d) It can be used to prevent packet looping.

(GATE 2010: 1 Mark)

Solution: Value of TTL is decremented to prevent packet looping.

Ans. (d)

46. Which one of the following is not a client–server application?

(a) Internet chat (b) Web browsing
(c) E-mail (d)Ping

(GATE 2010: 1 Mark)

Solution: ping is a command not an application. It is to check connectivity and there is no need to communicate with server.

Ans. (d)

47. Suppose computers A and B have IP addresses 10.105.1.113 and 10.105.1.91, respectively, and they both use the same net mask N. Which of the values of N given below should not be used if A and B should belong to the same network?

(a) 255.255.255.0 (b) 255.255.255.128
(c) 255.255.255.192 (d) 255.255.255.224

(GATE 2010: 2 Marks)

Solution: To belong to a different network, A and B should have different network address.

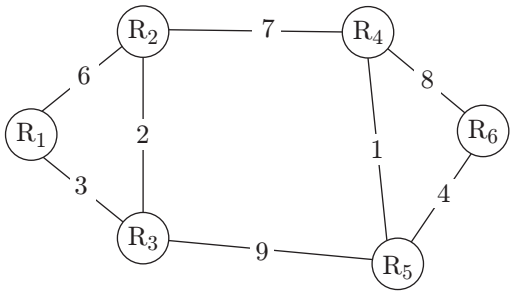
Perform logical AND operation on all the options.
For example,option (d)
IP address of A: 10.105.1. 01110001
Network mask: 255.255.255. 11100000
Network address of A: 10.105.1. 01100000

IP address of B: 10.105.1. 01011011
Network mask: 255.255.255. 11100000
Network address of A: 10.105.1. 01000000

Both have different network addresses.

Ans. (d)

Linked Answer Questions 48 and 49: Consider a network with 6 routers R_1 to R_6 connected with links having weights as shown in the following diagram



48. All the routers use the distance vector based routing algorithm to update their routing tables. Each router starts with its routing table initialised to contain an entry for each neighbour with the

weight of the respective connecting link. After all the routing tables stabilise, how many links in the network will never be used for carrying any data?

(a) 4 (b) 3 (c) 2 (d) 1

(GATE 2010: 2 Marks)

Solution: We can check one by one all shortest distances. When we check for all shortest distances for R_i we don't need to check its distances to R_0 to R_i-1 because the network graph is undirected. Following will be distance vectors of all nodes.

Shortest distances from R_1 to R_2, R_3, R_4, R_5 and R_6
R_1 (5, 3, 12, 12, 16)
Links used: R_1–R_3, R_3–R_2, R_2–R_4, R_3–R_5, R_5–R_6

Shortest distances from R_2 to R_3, R_4, R_5 and R_6
R_2 (2, 7, 8, 12)
Links used: R_2–R_3, R_2–R_4, R_4–R_5, R_5–R_6

Shortest distances from R_3 to R_4, R_5 and R_6
R_3 (9, 9, 13)
Links used: R_3–R_2, R_2–R_4, R_3–R_5, R_5–R_6

Shortest distances from R_4 to R_5 and R_6
R_4 (1, 5)
Links used: R_4–R_5, R_5–R_6

Shortest distance from R_5 to R_6
R_5 (4)

Links used: R_5–R_6

If we mark all the used links one by one, we can see that following links are never used.
R_1–R_2 R_4–R_6

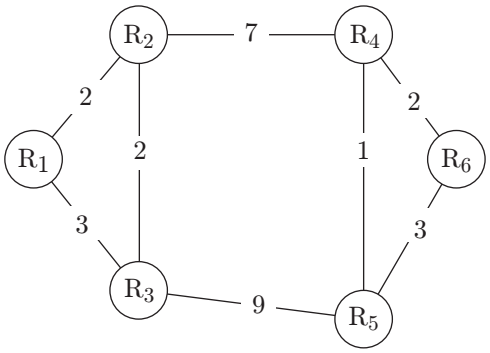
Ans. (c)

49. Suppose the weights of all unused links in the previous question are changed to 2 and the distance vector algorithm is used again until all routing tables stabilise. How many links will now remain unused?

(a) 0 (b) 1 (c) 2 (d) 3

(GATE 2010: 2 Marks)

Solution: After the weights of unused links() are changed to following graph.



Following will be distance vectors of all nodes
R_1 (2, 3, 9, 10, 11)
Links used: R_1–R_2, R_1–R_3, R_2–R_4, R_4–R_5, R_4–R_6
R_2 (2, 7, 8, 9)
Links used: R_2–R_3, R_2–R_4, R_4–R_5, R_4–R_6
R_3 (9, 9, 11)
Links used: R_3–R_2, R_2–R_4, R_3–R_5, R_4–R_6
R_4 (1, 2)
Links used: R_4–R_5, R_4–R_6
R_5 (3)
Links used: R_5–R_4, R_4–R_6
If we mark all the used links one by one, we can see that following links are never used.
R_5–R_6

Ans. (b)

50. A layer-4 firewall (a device that can look at all protocol headers up to the transport layer) CANNOT

(a) Block entire HTTP traffic during 9:00PM and 5:00 AM
(b) Block all ICMP traffic
(c) Stop incoming traffic from a specific IP address but allow outgoing traffic to the same IP address
(d) Block TCP traffic from a specific user on a multi-user system during 9:00 PM and 5:00 AM

(GATE 2011: 1 Mark)

Solution: As Layer-4 firewall cannot block traffic of Layer-5 (application layer) and HTTP is an application layer protocol. So, option (a) is correct.

Ans. (a)

51. Consider different activities related to email.

m_1: Send an email from a mail client to a mail server
m_2: Download an email from mailbox server to a mail client
m_3: Checking email in a web browser

Which is the application level protocol used in each activity?

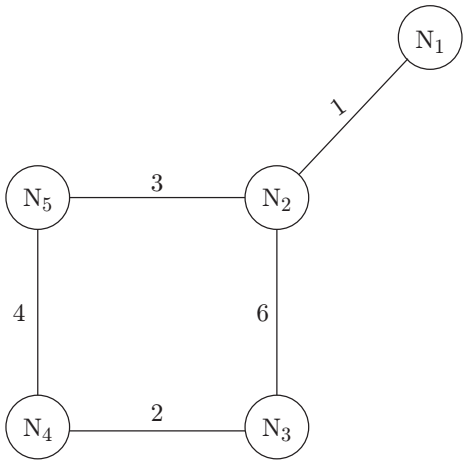
(a) m_i: HTTP m_2: SMTP m_3: POP
(b) m_i: SMTP m_2: FTP m_3: HTTP
(c) m_i: SMTP m_2: POP m_3: HTTP
(d) m_i: POP m_2: SMTP m_3: IMAP

(GATE 2011: 1 Mark)

Solution:
m_1: SMTP is responsible for mail transfer.
m_2: POP is responsible for downloading mail from mailbox server to mal client.
m_3: HTTP is responsible for viewing application on web browser.

Ans. (c)

Linked Answer Questions 52 and 53: Consider a network with five nodes, N_1 to N_5, as shown below.



The network uses a distance vector routing protocol. Once the routes have stabilised, the distance vectors at different nodes are as follows:

N_1:(0,1, 7, 8, 4) N_2: (1, 0, 6, 7, 3)
N_3: (7, 6, 0, 2, 6) N_4: (8,7, 2,0,4)
N_5: (4, 3, 6, 4, 0)

Each distance vector is the distance of the best-known path at that instance to nodes, N_1 to N_5, where the distance to itself is O. Also, all links are symmetric and the cost is identical in both directions. In each round, all nodes exchange their distance vectors with their respective neighbours. Then all nodes update their distance vectors. In between two rounds, any change in cost of a link will cause the two incident nodes to change only that entry in their distance vectors.

52. The cost of link N_2–N_3 reduces to 2 (in both directions). After the next round of updates, what will be the new distance vector at node N_3?

(a) (3, 2, 0, 2, 5) (b) (3, 2, 0, 2, 6)
(c) (7, 2, 0, 2, 5) (d) (7, 2, 0, 2, 6)

(GATE 2011: 2 Marks)

Solution: N_3: (3, 2, 0, 2, 5)

Ans. (a)

53. After the update in the previous question, the link N_1–N_2 goes down. N_2 will reflect this change immediately in its distance vector as cost, ∞. After the NEXT ROUND of update, what will be the cost to N_1 in the distance vector of N_3?

(a) 3 (b) 9 (c) 10 (d) ∞

(GATE 2011: 2 Marks)

Solution: N_3 to N_1 either by N_2 or by N_4

N_2–N_1 is ∞, so N_3 will choose to go via N_4 to N_1 $(2 + 8)$.

Ans. (c)

54. Which of the following transport layer protocols is used to support electronic mail?

(a) SMTP (b) IP (c) TCP (d) UDP

(GATE 2012: 1 Mark)

Solution: Electronic mail does not require TCP connection between sender and receiver of email.

Ans. (c)

55. The protocol data unit (PDU) for the application-layer in the Internet stack is

(a) segment. (b) datagram.
(c) message. (d) frame.

(GATE 2012: 1 Mark)

Solution:
The protocol data unit (PDU) for Data link layer = Frame; Network layer = Datagram; Transport layer = Segment; Application layer = Message.

Ans. (c)

56. In the IPv4 addressing format, the number of networks allowed under class C addresses is

(a) 2^{14} (b) 2^7 (c) 2^{21} (d) 2^{24}

(GATE 2012: 1 Mark)

Solution:

Network bits	Host bits
24 bits	8 bits

Starting with 3 bits (110) reserved to recognise the class. So, the number of networks are 2^{21}.

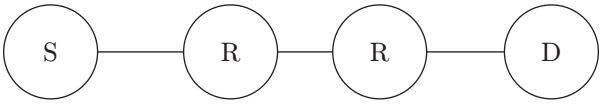
Ans. (c)

57. Consider a source computer (S) transmitting a file of size 10^6 bits to a destination computer (D) over a network of two routers (R_1 and R_2) and three links (L_1, L_2, and L_3). L_1 connects S to R_1; L_2 connects R_1 to R_2; and L_3 connects R_2 to D. Let each link be of length 100 km. Assume signals travel over each link at a speed of 10^8 meters per second. Assume that the link bandwidth on each link is 1Mbps. Let the file be broken down into 1000 packets each of size 1000 bits. Find the total sum of transmission and propagation delays in transmitting the file from S to D?

(a) 1005 ms (b) 1010 ms
(c) 3000 ms (d) 3003 ms

(GATE 2012: 2 Marks)

Solution



Transmission delay for 1 packet from each of S, R_1 and R_2 will take 1ms.

Propagation delay on L_1, L_2 and L_3 for one packet is 1 ms.
Transmission delay + Propagation delay = 2 ms
First packet will reach at 6th ms
Second packet will reach at 7th ms
1000 packets will reach at 1005th ms

Ans. (a)

58. Consider an instance of TCP's Additive Increase Multiplicative Decrease (AIMD) algorithm where the window size at the start of the slow start phase is 2 MSS and the threshold at the start of the first transmission is 8 MSS. Assume that a timeout occurs during the fifth transmission. Find the congestion window size at the end of the tenth transmission.

(a) 8 MSS (b) 14 MSS
(c) 7 MSS (d) 12 MSS

(GATE 2012: 2 Marks)

Solution:
In slow start, with each iteration, size of congestion window doubles. So,

T = 1 ws = 2
T = 2 ws = 4
T = 3 ws = 8

Threshold is 8. So now window size will increase by one using additive increase method.

T = 4 ws = 9
T = 5 ws = 10, here timeout occurs.

Hence, threshold = 10/2 = 5, ws is reset

T = 6 ws = 2
T = 7 ws = 4
T = 8 ws = 5 [threshold was 5, so apply additive increase]
T = 9 ws = 6
T = 10 ws = 7

Ans. (c)

59. An Internet Service Provider (ISP) has the following chunk of CIDR-based IP addresses available with it: 245.248.128.0/20. The ISP wants to give half of this chunk of addresses to organisation A, and a quarter to organisation B, while retaining the remaining with itself. Which of the following is a valid allocation of addresses to A and B?

(a) 245.248.136.0/21 and 245.248.128.0/22
(b) 245.248.128.0/21 and 245.248.128.0/22
(c) 245.248.132.0/22 and 245.248.132.0/21
(d) 245.248.136.0/24 and 245.248.132.0/21

(GATE 2012: 2 Marks)

Solution: Total numbers of addresses available are 4096.

Organisation A : 2048
Organisation B : 1024
Remaining : 1024

Allocation of addresses to A: 11 bits are required for organisation A.

245.248. 10000	100.00000000

Address allocated is 245.248.136.0/21
Allocation of addresses to B: 10 bits are required for organisation B.

245.248. 100000	00.00000000

Address allocated is 245.248.128.0/22.

Ans. (a)

60. The transport layer protocols used for real time multimedia, file transfer, DNS and email, respectively, are

(a) TCP, UDP, UDP and TCP
(b) UDP, TCP, TCP and UDP
(c) UDP, TCP, UDP and TCP
(d) TCP, UDP, TCP and UDP

(GATE 2013: 1 Mark)

Solution: Real-time multimedia: UDP (session less protocol, used where fast data transfer is required)

File transfer: TCP
DNS: UDP
E-mail: TCP

Ans. (c)

61. Using public key cryptography, X adds a digital signature σ to message M, encrypts $< M, \sigma >$, and sends it to Y, where it is decrypted. Which one of the following sequences of keys is used for the operations?

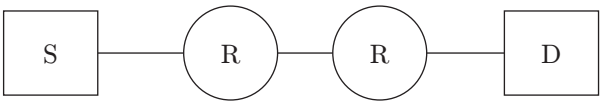
(a) Encryption: X's private key followed by Y's private key; Decryption: X's public key followed by Y's public key
(b) Encryption: X's private key followed by Y's public key; Decryption: X's public key followed by Y's private key
(c) Encryption: X's public key followed by Y's private key; Decryption: Y's public key followed by X's private key
(d) Encryption: X's private key followed by Y's public key; Decryption: Y's private key followed by X's public key

(GATE 2013: 1 Mark)

Solution: X uses private key to add digital signature, then uses Y's public key to encrypt. On the other end, Y first uses its private key followed by X's public key.

Ans. (d)

62. Assume that source S and destination D are connected through two intermediate routers labelled R.



Determine how many times each packet has to visit the network layer and the data link layer during a transmission from S to D.

(a) Network layer – 4 times and Data link layer – 4 times
(b) Network layer – 4 times and Data link layer – 3 times
(c) Network layer – 4 times and Data link layer – 6 times
(d) Network layer – 2 times and Data link layer – 6 times

(GATE 2013: 1 Mark)

Solution: Transmission from S to D will follow these steps:

At S: Network layer → Data link layer
At R1: Data link layer → Network layer → Data link layer
At R2: Data link layer → Network layer → Data link layer
At D: Data link layer → Network layer
Therefore, the packet has to visit 6 times data link layer and 4 times network layer.

Ans.(c)

63. Determine the maximum length of the cable (in km) for transmitting data at a rate of 500 Mbps in an Ethernet LAN with frames of size 10000 bits. Assume the signal speed in the cable to be 200000 km/s.

(a) 1 (b) 2
(c) 2.5 (d) 5

(GATE 2013: 2 Marks)

Solution: Data rate: 500 Mbps = 5×10^8 bps
Frame size: 10000 bits

Speed: 200000 km/s

$$5 \times 10^8 \text{ bits can travel} = 1\text{s}$$

$$10^4 \text{ bits will travel} = \frac{10^4}{5\times10^8} = \frac{1}{5\times10^4}$$

In 1 s, distance travelled = 2×10^5 km

$$\text{In } (1/5 \times 10^4) \text{ s, distance travelled is} = \frac{2\times10^5}{5\times10^4} = 4 \text{ km}$$

Hence, the maximum distance is $4/2 = 2$ km

Ans. (b)

64. In an IPv4 datagram, the M bit is 0, the value of HLEN is 10, the value of total length is 400 and the fragment offset value is 300. The position of the datagram, the sequence numbers of the first and the last bytes of the payload, respectively, are

(a) Last fragment, 2400 and 2789
(b) First fragment, 2400 and 2759
(c) Last fragment, 2400 and 2759
(d) Middle fragment, 300 and 689

(GATE 2013: 2 Marks)

Solution: $M = 0$ indicates no more fragment means last fragment

Actual header length is $4 \times 10 = 40$
Total length = 400 bytes (40-byte header + 360-byte payload)
Fragment offset = $300 \times 8 = 2400$ bytes (measured in terms of 8 bytes)
First byte sequence number of last fragment is 2400.
Sequence number of last byte payload is $2400 + 360 - 1 = 2759$.

Ans. (c)

PRACTICE EXERCISES

Set 1

1. Which layer is associated with log in/log out from the network?

(a) Transport (b) Presentation
(c) Data link (d) Session

2. Which layer is associated with IP addresses?

(a) Session (b) Network
(c) Transport (d) Data link

3. The size of MAC address and IPv4 address is

(a) 8 bits and 24 bits (b) 32 bits and 48 bits
(c) 48 bits and 32 bits (d) 24 bits and 32 bits

4. The bit size of cyclic redundancy code in an Ethernet is

(a) CRC is not used in Ethernet
(b) 8
(c) 24
(d) 32

5. MTU stands for

(a) Minimum Transfer Unit
(b) Minimum Telephony Unit
(c) Maximum Transfer Unit
(d) Memory Transfer Unit

6. Using 7-bit sequence number, what is the maximum size (in bits) of the sender and receiver window using Go-Back-N ARQ?

(a) 127 and 1 (b) 1 and 127
(c) 127 and 127 (d) 1 and 1

7. Using a 5-bit sequence number, what is the maximum size of the sender and receiver window using selective repeat ARQ?

(a) 16 and 16 (b) 1 and 16
(c) 16 and 1 (d) Depend upon the bits selected to be repeated

8. Which protocol is being used in wireless to overcome collision?

(a) CSMA/CD
(b) CSMA/CA
(c) Both
(d) WEP

9. The host bits present in class B IP address are _____.

10. Which protocol is used to provide error reporting services to IP address?

(a) ICMP (b) ARP
(c) BGP (d) OSPF

11. Which protocol is used to find the physical address for a logical address?

(a) ARP (b) RARP
(c) IGMP (d) ICMP

12. Which protocol cannot be used to find the logical address if the server is residing out of your network?

(a) ARP (b) RARP
(c) BOOTP (d) IGMP

13. Which topology requires a central controller or hub?

(a) Bus (b) Star
(c) Mesh (d) Ring

14. The number of nibbles are reserved in the IP header for header length is _____.

15. How many hops can be travelled by the IP packet having TTL value 5?

(a) It cannot travel any hop.
(b) It can travel only single hop.
(c) It can travel five hops.
(d) It can travel four hops.

16. What does the acronym ISDN for?

(a) Indian Standard Data Network
(b) Integrated Services Digital Networks
(c) Intelligent Secure Digital Network
(d) Intelligent Services Digital Network

17. If N is the maximum sequence number, then the window size in selective repeat and Go-Back-N protocols are, respectively,

(a) N/2, N − 1 (b) N/2, N + 1
(c) N + 1/2, N − 1/2 (d) N − 1, N

18. CRC can detect all burst error of up to M errors, if generator polynomial $G(x)$ is of degree

(a) It does not matter (b) $M - 1$
(c) $M/2$ (d) $M + 1$

19. Which layers of the OSI reference model are host-to-host layers?

(a) Transport, session, presentation, application
(b) Session, presentation, application
(c) Datalink, transport, presentation, application
(d) Physical, datalink, network, transport

20. A nibble is used for packed sequence numbering in a sliding window protocol used in a computer network. What is the maximum window size?

(a) Depends upon the underlying network protocol
(b) Depends upon the number of nodes involved in the network
(c) 15
(d) 16

21. Infrared signals can be used in a closed area using _____ propagation.

(a) Sky (b) Ground
(c) Line of sight (d) Small signal

22. A bridge has access to _____ address in the same network.

(a) Physical (b) Logical
(c) Supernet (d) Link state

23. Match the following:

List – I	List – II
A. Physical layer	i. Resources to network access are used
B. Data link layer	ii. Packets are moved from one destination to other
C. Network layer	iii. Process to process message delivery
D. Transport layer	iv. Bit stream is transmitted
E. Application Layer	v. Frames are formed

Codes:

	A	B	C	D	E
(a)	iv	v	ii	iii	i
(b)	i	iii	iv	ii	v
(c)	iv	ii	i	v	iii
(d)	i	ii	iii	iv	v

24. The _____ is a unit to measure the signal strength in wireless networks

(a) Frequency (b) Bandwidth delay product
(c) Attenuation (d) Decibel

25. Which one of the following media is multi-drop?

(a) UTP cable (b) STP cable
(c) Thick coaxial cable (d) Multi-mode fibre optic cable

26. What is the baud rate of the standard 20 Mbps Ethernet?

(a) 10 megabaud (b) 40 megabaud
(c) 30 megabaud (d) 20 megabaud

27. Binary symmetric channel uses

(a) half-duplex protocol
(b) full-duplex protocol
(c) simplex protocol
(d) simplex protocol with separate data and control bits

28. Which of the following addresses is used to deliver a message to the correct application program running on a host?

(a) Port (b) DNS address
(c) Logical address (d) MAC address

29. Which of the following protocol is used for performing RPCs between applications in a language and system in an independent way?

(a) DHCP (b) SNMP
(c) SOAP (d) SMTP

30. Which layer of OSI reference model is responsible for decomposition of messages and generation of sequence numbers to ensure correct re-composition from end-to-end communication in a network?

(a) Physical (b) Session
(c) Transport (d) Data link

31. The VLF and LF bauds use _____ propagation for communication.

(a) Ground (b) Sky
(c) Line of sight (d) Space

32. Using the 8-bit sequence numbers, what is the maximum size of the sender and receiver window in selective repeat ARQ?

(a) 128 and 128
(b) 1 and 127
(c) 128 and 127
(d) 8 and 8

33. Vulnerable Slotted ALOHA is

(a) equal to average frame transmission time
(b) half of average frame transmission time
(c) two times the average frame transmission time
(d) none

34. A CSMA/CD network supports data rate of 10Mbps, the maximum distance between any two stations is found to be 2500 m for the correct operation of the collision detection process. What should be the maximum distance if the data rate is increased to 100 Mbps?

(a) 25000 m (b) 2500 m
(c) 250 m (d) 25 m

35. Consider an IP in CIDR notation as 220.19.18.87/24. The first and the last address of this network will be?

(a) 220.19.18.24 and 220.19.18.87
(b) 220.19.18.0 and 220.19.18.87
(c) 220.19.18.0 and 220.19.18.123
(d) 220.19.18.0 and 220.19.18.255

36. In ICMP, 8 byte of the IP datagram is included in ICMP data part because:

(a) It contains the IP address.
(b) It contains the port numbers.
(c) The statement is false, IP datagram is not included in ICMP data part.
(d) It is helpful in checking the errors with CRC used.

37. A receiver receives the IP packet with the first 8 bits as 10100011. The length of the IP packet is

(a) 163 bytes (b) 1 byte
(c) 127 bytes (d) 12 bytes

38. The router performs at _____ layer(s).

(a) Only physical
(b) Physical, datalink and network
(c) Physical, datalink and transport
(d) Datalink and network

39. A packet has arrived with the offset value 100 and HLEN value 5. The total length value is 100. What is the number of first byte and the last byte?

(a) 879 (b) 880
(c) 881 (d) 882

40. Which of the following is true?

(a) In TCP/IP-based services, the destination address is to be specified only during the initial stage of setup.
(b) Initial setup is required for UDP-based service.
(c) Packet sequencing is not guaranteed in TCP/IP-based services.
(d) Initial setup is not possible in UDP-based service.

41. How many characters (7 bits + 1 parity) can be transmitted over 2400 bps line, if the transfer is asynchronous (1 start and 1 stop)?

(a) 2400/8 (b) 2400/10
(c) $2400 \times 8/2$ (d) 256

42. In CRC, if the data unit is 110111001 and the divisor is 1011 then what is the dividend at the receiver?

(a) 110111001101
(b) 110111001000
(c) 110111001011
(d) 101110111001

43. With respect to ICMP, which of the following statements is false?

(a) ICMP reports about the routers.
(b) ICMP is also used to test connectivity.
(c) ICMP and BOOTP are equivalent in their usage.
(d) An ICMP message type is encapsulated for transmission.

44. A 3000-lm long trunk is used to transmit frames using Go-Back-N protocol. The propagation speed is 6 μs/km and the trunk data rate is 1.544 Mbps. We ignore the time it takes to receive the acknowledgement bits. Frame size is 64 bytes. What should be the maximum window size at the sender's side in order to achieve 100% efficiency?

(a) 3000 (b) 1544
(c) 110 (d) 64

45. In a pure ALOHA network, 100 stations share a link of 1 Mbps. The throughput of such a network having 1000 bits size of frames and each station is transmitting at the rate of 10 frames/s is

(a) 10% (b) 13.53%
(c) 12.8% (d) 18.16%

46. An HDLC does not support

(a) simplex
(b) multipoint link
(c) balanced multipoint
(d) full duplex

47. A hub in the network is

(a) a passive device
(b) an active device
(c) a server that serves every node
(d) a power supply concentrator

48. Consider the following message: $M = 1010001101$. The CRC of this message using the divisor polynomial $x^5 + x^4 + x^2 + 1$ is

(a) 1110 (b) 0101
(c) 1001 (d) 0010

49. The broadcast address for the subnet that IP address 192.168.26.8, 255.255.255.248 is a member of

(a) 192.168.26.225 (b) 192.168.26.255
(c) 192.168.127.255 (d) 192.168.26.0

50. A sender uses public key cryptography to send a secret message. Which of the following is true?

(a) Sender encrypts using receiver's public key
(b) Sender encrypts using his own public key
(c) Receiver decrypts using sender's private key
(d) Receiver decrypts using own private key

51. Which of the following functionality must be implemented by transport layer over and above the network protocol?

(a) Recovery from packet loss
(b) End to end connectivity
(c) Packet delivery in encapsulated abstract order
(d) Secure transmission from end to end

52. During the process of packet forwarding by the routers, _____ field is not updated.

(a) IP header source address
(b) IP header target address
(c) IP header TTL
(d) IP header checksum

53. Consider the network, using CIDR addressing, a PC having the IP address as 180.10.10.10/20. The numbers of addresses in such a network will be _____ ?

(a) 255 (b) 4094 (c) 4096 (d) 1024

Set 2

1. Consider the following two cases given below, where G denotes the generator polynomial and M denotes the received message:

Case 1: $G = 1100$, $M = 1010101$
Case 2: $G = 11001$, $M = 111000111011$
In which transmissions errors occur?

(a) 1 only (b) 2 only
(c) Both 1 and 2 (d) Neither 1 nor 2

2. A block of addresses is granted to a small organisation. We have given a random address 216.18.9.21/28.

What is the first address in the block?

(a) 216.18.9.0 (b) 216.18.9.16
(c) 216.18.9.18 (d) 216.18.9.21

3. How many total numbers of addresses are there in the block using the information in the above question?

(a) 16 (b) 32 (c) 64 (d) 128

4. A channel has 10 Kbps bit rate using stop-and-wait protocol and has propagation delay of 5 ms. For a frame with 360 bit, what will be the efficiency?

(a) 92% (b) 88%
(c) 84% (d) 78%

5. Consider a 3 Mbps token ring LAN and frame size is of 200 byte. If the ring latency is 150 μs, then what will be the effective data rate of the LAN?

(a) 2.10 Mbps (b) 2.25 Mbps
(c) 2.35 Mbps (d) 2.90 Mbps

6. Host A is sending data to host B over a full duplex link. A and B are using the sliding window protocol for flow control. The send and receive window sizes are 6 packets each. Data packets (sent only from A to B) are all 1000 bytes long and the transmission time for such a packet is 40 μs. Acknowledgement packets (sent only from B to A) are very small and require negligible transmission time. The propagation delay over the link is 180 μs. What is the maximum achievable throughput in this communication?

(a) 14.28×10^6 bps (b) 14.61×10^6 bps
(c) 19.33×10^6 bps (d) 23.40×10^6 bps

7. Station A uses 32 bytes packets to transmit messages to station B using a sliding window protocol. The round-trip delay between A and B is 60 ms and the bottleneck bandwidth on the path between A and B is between 128 Kbps. What is the optimal window size that A should use?

(a) 20 (b) 30
(c) 60 (d) 40

8. Frames of 1000 bits are sent over a 10^6 bps duplex link between the two hosts. The propagation time is 34 ms. Frames are to be transmitted into this link to maximally pack them in transit (within the link). What is the minimum number of bits (l) that will be required to represent the sequence of numbers distinctly? Assume that no time gap needs to be given between transmissions of two frames.

(a) $l = 4$ (b) $l = 5$
(c) $l = 6$ (d) $l = 7$

9. A 3-km long broadcast LAN has 10^7 bps bandwidth and uses CSMA/CD. The signal travels along the wire at 4×10^8 m/s. What is the minimum packet size that can be used on this network?

(a) 50 bytes (b) 100 bytes
(c) 200 bytes (d) None of these

10. Match the following:

(A) 204.26.37.47	i. Class A
(B) 145.12.13.0	ii. Class B
(C) 230.54.256.56	iii. Class C
(D) 255.255.255.255	iv. Class D
(E) 126.126.126.126	v. Class E
(F) 85.18.257.24	vi. Invalid IP

(a) A-iv	B-ii	C-iv	D-v	E-i	F-i
(b) A-iii	B-ii	C-vi	D-v	E-i	F-vi
(c) A-iii	B-ii	C-iv	D-iv	E-vi	F-i
(d) A-iii	B-ii	C-iv	D-vi	E-i	F-vi

11. In a class C network if subnet mask is given as 255.255.255.224. Calculate the number of subnet and number of host in each subnet (practically possible).

(a) 4 and 32 (b) 6 and 64
(c) 8 and 32 (d) 6 and 30

12. We need to make a super network out of 16 class C block, what is the supernet mask?

(a) 255.255.255.240
(b) 255.240.0.0
(c) 255.255.240.0
(d) 255.255.224.0

13. Given that bandwidth = 10 Mbps, distance = 4 km and velocity = 2×10^8 m/s. The number of bits are transmitted in RTT is _____.

14. Suppose the round-trip propagation delay for a 8 Mbps Ethernet having 48-bit jamming signal is 50 μs. The minimum frame size is _____.

15. The address of a class B host is to be split into subnets with a 7-bit subnet number. What is the maximum number of subnets and the maximum number of hosts in each subnet?

(a) 128 subnets and 1024 hosts
(b) 128 subnets and 1022 hosts
(c) 126 subnets and 512 hosts
(d) 126 subnets and 510 hosts

16. If a class B network on the Internet has a subnet mask of 255.255.248.0, what is the maximum number of hosts per subnet?

(a) 1022 (b) 1023
(c) 2046 (d) 2047

17. In a network,propagation delay is 100 μs and bandwidth is given as 100 Mbps. Calculate how many RTTs are required for transmitting 40000 bits in stop-and-wait ARQ.

(a) 2 (b) 4 (c) 7 (d) 9

18. If 5-bit sequence number is used, what is the sequence number after sending 100 frames in Go-Back-N ARQ?

(a) 2 (b) 3 (c) 4 (d) 5

19. If N is a maximum sequence number in sliding window of Go-Back-N ARQ. How many sequence bit will be there for use?

(a) $\log_2 N$ (b) $1/\log_2 N$
(c) $\log_2 N^2$ (d) $\log_2 N + 1$

20. If 6 bits are used for sequence number, then what is the sender window size and receiver window size in selective repeat scheme?

(a) 64 (b) 63
(c) 32 (d) 31

21. If 10 Base 5 cable is used and velocity is 2×10^8 m/s. What will be the frame size in CSMA/CD?

(a) 40 (b) 50
(c) 60 (d) 64

22. If the capacity of a router is 1.2 mb, output rate of data is .8 mb/s token that are generated is 6 mb/s. Calculate the time matrix busted traffic is routed.

(a) 0.6 s (b) 1.2 s
(c) 1.5 s (d) 2.0 s

23. If the total length bits are 0000000000111111 and HLEN = 1010, then which one is true about the size of header and payload?

(a) 40 and 63
(b) 40 and 23
(c) 24 and 63
(d) 24 and 23

24. In ICMP protocol, error reporting message type 11 denotes which of the message type?

(a) Destination unreachable
(b) Source quench
(c) Time exceeded
(d) Parameter problem

25. In a token ring network, the transmission speed is 32 bps and the propagation speed is 200 m/μs. The 4-bit delay in this network is equivalent to:

(a) 12 m of cable (b) 18 m of cable
(c) 22 m of cable (d) 25 m of cable

ANSWERS TO PRACTICE EXERCISES

Set 1

1. (d)	**8.** (b)	**15.** (c)	**22.** (a)	**29.** (c)	**36.** (b)	**43.** (c)	**50.** (a)
2. (b)	**9.** (16)	**16.** (b)	**23.** (a)	**30.** (c)	**37.** (d)	**44.** (c)	**51.** (b)
3. (c)	**10.** (a)	**17.** (a)	**24.** (d)	**31.** (a)	**38.** (b)	**45.** (b)	**52.** (b)
4. (d)	**11.** (a)	**18.** (d)	**25.** (c)	**32.** (a)	**39.** (a)	**46.** (c)	**53.** (b)
5. (c)	**12.** (b)	**19.** (a)	**26.** (b)	**33.** (a)	**40.** (d)	**47.** (a)	
6. (a)	**13.** (b)	**20.** (c)	**27.** (a)	**34.** (c)	**41.** (b)	**48.** (d)	
7. (a)	**14.** (4)	**21.** (c)	**28.** (a)	**35.** (d)	**42.** (c)	**49.** (b)	

Set 2

1. (a) In case 1: when M (1010101) by G (1100), we will get remainder which do not have all zeros.

In case 2: when M (111000111011) by G (11001), we will get all zeros in remainder.

2. (b) One network address: 216.18.9.21

Subnet mask: 255.255.255.240
By doing XOR between network id and subnet mask, we get first address of block = 216.18.9.16.

3. (a) Total number of addresses $= 2^{32-28} = 2^4 = 16$

4. (d) Transmission time $= \dfrac{\text{Data size}}{\text{Bandwidth}} = \dfrac{360}{10000} = 36$ ms

Utilization in percentage

$$= \frac{\text{Transmission time}}{\text{Transmission time} + (2 \times \text{Propagation time})} \times 100$$

$$= \frac{36}{36+10} \times 100 = 78.2 \approx 78\%$$

5. (c) Transmission time $= \dfrac{\text{Data size}}{\text{Bandwidth}} = \dfrac{200 \times 8}{3 \times 10^6}$

$= 0.00053$ s

Ring latency = Round-trip time = 150 μs = 0.00015 s
Total time required to transfer 1600 bits = (0.00053 + 0.00015) = 0.00068 s
So, effective data rate = 1600/0.00068 = 2.35 Mbps

6. (a) We have

Window size (n) = 6 packets
Packet size = 1000 bytes
So, total packet size = 6 × 1000 = 6000 bytes
Total time = Transmission time + Propagation time
$= 6 \times 40 + 180$ μs $= 420$ μs $= 420 \times 10^{-6}$s

$$\text{Maximum achievable throughput} = \frac{\text{Total size}}{\text{Total time}}$$

$$= \frac{6000}{420 \times 10^{-6}} = \frac{6000 \times 10^6}{420}$$

$= 14.28 \times 10^6$ bps

7. (b) Given round-trip delay (T) = 60 ms = 60×10^{-3}s

$R = 128$ Kbps $= 128 \times 10^3$ bps
$L = R \times T = 128 \times 10^3 \times 60 \times 10^{-3} = 128 \times 60$

$$\text{So, optional window size } (n) = \frac{128 \times 60}{32 \times 8}$$

$$= \frac{7680}{256} = 30$$

8. (c) Because of duplex link we need not wait for twice the propagation time for sending the frame. If the sender window size is N, then

Transmitting 10^6 bits require = 1 s
Therefore, $N \times 10^{-3}$ s = N ms
Therefore, N ms = 34 ms, $N = 34 < 2^6$
So, minimum number of bits required is 6.

9. (d) In CSMA/CD, the minimum frame size = $2 \times z \times$ bandwidth

Given that distance (d) = 3 km = 3×10^3 m, velocity (v) = 4×10^8 m/s and bandwidth = 10^7 bps.
Therefore, minimum pocket size

$= 2 \times (7.5 \times 10^{-6}) \times 10^7 = 2 \times 7.5 \times 10$
$= 150$ bits $= 150/8 \approx 19$ bytes

10. (b) Number greater than 255 is not allowed in valid IP. In option (f), 3rd octave has 257 value which is not valid. So, option (f) should match (vi). Similarly, option (c) should match (vi).

11. (d) Subnetmask 255.255.255.224 – 11111111. 11111111. 11111111. 11100000

Number of subnet = $2^3 - 2 = 6$
Number of host in each subnet = $2^5 - 2 = 30$
Two addresses are reduced because one is for network address and another is for broadcasting.

12. (c) Default mask of

class C = 255.	255.	255.	0
11111111	11111111	11111111	00000000

Required 16 class C blocks, so

11111111	11111111	1111<u>0000</u>	00000000

We have used last 4 bit for combining 16 class C blocks. So supernet mask is {255.255.240.0}

13. (400) RTT (round-trip time) = 2× PT (propagation time)

$$\text{Propagation time (PT)} = \frac{\text{Distance}}{\text{Velocity}} = \frac{4 \times 10^3}{2 \times 10^8}$$

$$= 2 \times 10^{-5}\text{s} = 20\ \mu\text{s}$$

RTT = 2 × PT = 2 × 20 = 40 μs
For 1 s, bits transmitted = 10^7 bits
So, for 40 μs, the buts transmitted = $40 \times 10^{-6} \times 10^7 = 400$ bits

14. (400) Frame size = $(2T_P) \times$ (Bandwidth) = 50 ms × 8 Mbps = 400 Kbits

15. (d) The Class B is defined as follows

Network id = 16 bit
Host id = 16 bit

Maximum number of subnets
$= 2^7 - 2 = 128 - 2 = 126$
Maximum number of hosts in each subnet
$= 2^{16} - 7 - 2 = 2^9 - 2 = 510$

16. (c) Generally, the number of addresses usable for addressing specific hosts in each network is always $2^N - 2$, where N is the number of bits for host id.

The binary representation of subnet mask is 11111 111.11111111.11111000.00000000.

There are 21 bits set in subnet. So, 11 (i.e., 32 − 21) bits are left for host ids.

Total possible values of host ids is $2^{11} = 2048$.

Out of 2048 values, 2 addresses are reserved.

The address with all bits as 1 is reserved as broadcast address and address with all host id bits as 0 is used as network address of subnet.

17. (a) Given that bandwidth = 100 Mbps = $100 \times 10^6 = 10^8$ bits and propagation time = 100 μs

We know that

$$\text{RTT} = 2 \times \text{PT} = 200\ \mu\text{s}$$
$$\text{Data transfer in 1 s} = 10^8$$

So, data transfer in 200 μs (in 1 RTT) = $200 \times 10^{-6} \times 10^8 = 20000$ bits
Required RTT for transmitting 40000 bits = 40000/20000 = 2

18. (b) Sequence bits (n) = 5
Maximum value of sequence number = $2^n - 1$

0	1	2	3	-	30	31	0	1	2	-	30	31	0	1	2	-	30	31	0	1	2	3
				-						-						-						
				-						-						-						
				-						-						-						

(0−30) = 31 frames
(31−29) = 31 frames
(30−28) = 31 frames
Total = 93 frames

Total frames left 6 and they will be counted as 29, 30, 31, 0, 1, 2.

So, after 99th frame, sequence number will be 3.

19. (d) If sequence bits are N, then maximum sequence number is = $2^N - 1$, so

Number of sequence bits = $\log_2 N + 1$

20. (c) If sequence bits are n, then window size = 2^{n-1}

So, for 6-bit sequence number, window size = $2^{6-1} = 2^5 = 32$

21. (b) Given that distance = 500 m and bandwidth = 10 Mbps

Frame transmission time = 2 × Propagation delay
Therefore,

$$\frac{\text{Frame size}}{\text{Bandwidth}} = 2 \times \frac{\text{Distance}}{\text{Velocity}}$$
$$\frac{\text{Frame size}}{10 \times 10^6\ \text{b/s}} = 2 \times \frac{500\ \text{m}}{2 \times 10^8\ \text{m/s}}$$

Frame size = 50 bits

22. (a) Formula to calculate time = $C + \rho S = MS$

where capacity (C) = 1.2×10^6, token generation rate (ρ) = 6 mb/s and output rate (M) = 8×10^6. Putting values into formula, we get

$$(1.2 \times 10^6) + 6 \times 10^6 \times S = (8 \times 10^6)\ S$$
$$10^6(1.2 + 6S) = (8 \times 10^6)\ S$$
$$S = \frac{1.2}{2} = 0.6\ \text{s}$$

23. (b) Packet size = $(0000000000111111)_2 = 63$

Header size = HLEN × 4 = 1010 × 4 = $(1010)_2 \times 4 = 40$
Packet size = Header + Payload
63 = 40 + Payload ⇒ Payload = 23

24. (c) Error message types

3→ destinations unreachable
4→ source quench
11→ time exceeded
12→ parameter problem

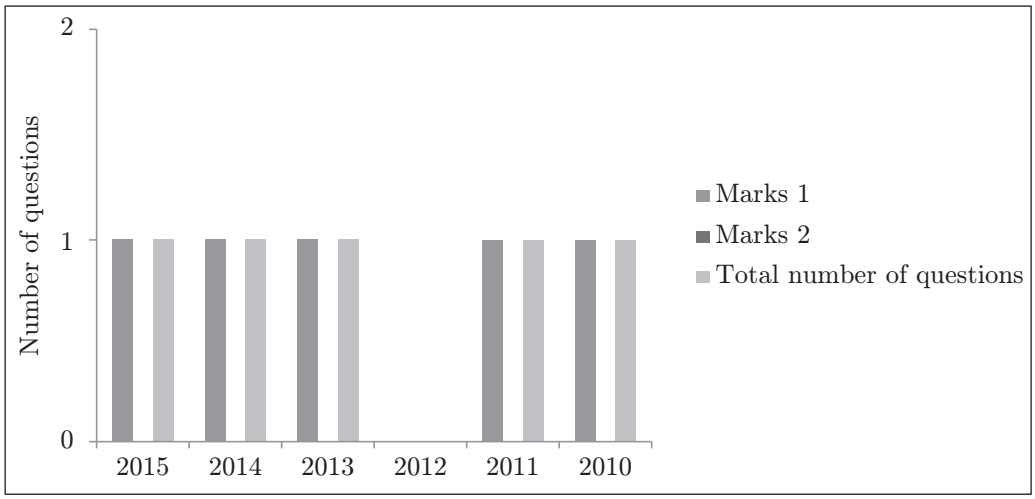
25. (d)

Given that $R = 32 \times 10^6$ bps, $B = 4$, $V = 200$ m/μs; d =?

$$d = \frac{Bv}{R} = \frac{4 \times 200}{32 \times 10^6 \times 10^{-6}} = 25\ \text{m of cable}$$

UNIT XI: WEB TECHNOLOGIES

LAST SIX YEARS' GATE ANALYSIS



Concepts on which questions were asked in the previous six years

Year	Concept
2015	Unix Sockets, XML and HTML
2014	HTML Web page and http server
2013	Communication technology
2012	Nil
2011	HTML elements
2010	Client–server application