GATE 2020
PSUs 2020

MADE EASY Publications

Revised & Updated Edition

POSTAL STUDY PACKAGE

COMPUTER SCIENCE & IT

Computer Networks

Objective Practice Sets

POSTAL Study Package 2020

Computer Science & IT

Objective Practice Sets

Computer Networks

Contents

MADE EASY Publications

1 CHAPTER
Networking Fundamentals and Physical Layer

1. Match the following groups based on layer of OSI model.

Group-1	Group-2
A. Hub	1. Physical layer
B. Bridge	2. Data link layer
C. Router	3. Network layer
D. Server	4. Application layer

Codes:

	A	B	C	D
(a)	1	2	3	4
(b)	2	2	3	3
(c)	2	3	3	3
(d)	1	3	3	4

2. Match the following groups

Group-1	Group-2
A. Link	1. Message
B. Network	2. Segment
C. Application	3. Datagram
D. Transport	4. Frame

Codes:

	A	B	C	D
(a)	3	4	2	1
(b)	4	3	2	1
(c)	4	3	1	2
(d)	3	4	1	2

3. A device which connects dissimilar LANs of different topologies using different sets of communication protocols so that information can flow from one to another is called
(a) Router (b) Bridge
(c) Gateway (d) Switch

4. Which of the following device is used to connect multiple devices to a network and does not stop broadcast traffic?
(a) Switch (b) Hub
(c) Modem (d) Repeater

5. Match List-I with List-II and select the correct answer using the codes given below the lists:

List-I
A. Route Determination
B. Flow Control
C. Interface to transmission media
D. Access for the end user

List-II
1. Data link and transport layer
2. Network layer
3. Application layer
4. Physical layer

Codes:

	A	B	C	D
(a)	1	2	3	4
(b)	1	2	4	3
(c)	2	1	3	4
(d)	2	1	4	3

6. Which of the following is not true?
(a) Ring topology of N-devices contains (N – 1) dropline and N-Ring cables.
(b) Bus topology of N-devices needs 1 dropline and N-Backbone cables.
(c) Star topology of N-devices contains N + 1 links and N-ports.
(d) All of these

7. Match the following:

List-I
A. Protocol converter
B. Passive device
C. It is a pure electronic device with no software
D. Retransmits the data with high signal without interpreting
E. Pure electronic device but associated with software
F. Active device used to connect multiple LANS with filtering and forwarding as main design criteria
G. Combination of bridge and router

List-II
1. Gateway
2. Brouter
3. Router
4. Bridge
5. Switch
6. Repeater
7. Hub

Codes:

	A	B	C	D	E	F	G
(a)	1	7	5	6	3	4	2
(b)	2	7	5	6	5	4	1
(c)	2	4	5	6	5	7	1
(d)	1	2	5	4	3	6	7

8. Consider the following statements regarding OSI model
(i) It divides the network communication into smaller and simpler components, aiding component development, design and troubleshooting.
(ii) It allows multiple-vendor development through standardization of network components.
(iii) It prevents the changes in one layer from affecting the other layers, allowing for quicker development.
(iv) It usually do not correspond exactly to the protocol stack running on an actual system.
Which of the above are true?
(a) (i) & (iv) only (b) (ii) and (iii) only
(c) (i), (ii) & (iv) only (d) All of these

9. The best effort delivery services such as an IP does not include
(a) error checking
(b) datagram acknowledgment
(c) error correction
(d) All of the above

10. The efficiency of Ethernet
(a) increases when propagation delay and transmission delays are low.
(b) increases when propagation delay is low and transmission delay is high.
(c) increases when propagation delay is high and transmission delay is low.
(d) increases when propagation delay and transmission delays are high.

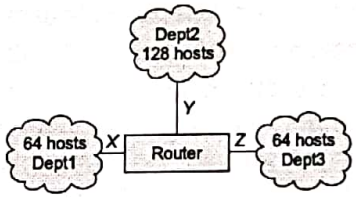
11. Match column A with column B:

Column-A	Column-B
A. DNS	1. Port - 20
B. POP3	2. Port - 21
C. FTP (Data)	3. Port - 53
D. FTP (Control)	4. Port - 110
	5. Port - 69

Codes:

	A	B	C	D
(a)	3	4	2	1
(b)	3	4	1	2
(c)	3	5	1	2
(d)	3	5	2	1

12. Considered the following router with three sub networks



Suppose if above network uses class C network 192.203.16.0 then find the subnet mask used for the department Y. [Assume all are in the same network].
(a) 255.255.255.0 (b) 255.255.255.128
(c) 255.255.255.192 (d) 255.255.255.255

13. In CIDR, if IP address is used 192.60.128.0/22. Then find the net mask?
(a) 255.255.255.0 (b) 255.255.252.0
(c) 255.255.255.128 (d) 255.255.128.0

14. Match the following:
List-I (Packets)

A.

	Source IP	Destination IP
Data	250.255.255.255	40.40.40.40

B.

	Source IP	Destination IP
Data	22.21.23.24	255.255.255.255

C.

	Source IP	Destination IP
Data	24.23.22.21	24.22.23.24

List-II
1. Unicast packet within network
2. This packet never exists
3. Limited broadcasting

Codes:

	A	B	C
(a)	1	2	3
(b)	2	3	1
(c)	3	1	2
(d)	2	1	3

15. To form supernetting
(a) All the network should be contigous
(b) Size of all network should be same (in power of 2)
(c) 1st Network ID is divisible by sir of all network
(d) All of the above

16. Which classful subnet mask is useful for need of subnet a network that has 5 subnets, each with at least 20 hosts.
(a) 255.255.255.192 (b) 255.255.255.248
(c) 255.255.255.240 (d) 255.255.255.224

17. On a class *B* network, total number of subnets are available with a subnet mask of 240.

18. A Network that is 172.28.0.0 and would like to support 650 hosts per subnet. The subnet mask should we use is 255.255. _____ and _____?

19. 32 bit IP address containing all 1's represent
(a) this computer (b) directed broadcast
(c) loop back (d) limited broadcast

20. The router connecting a company's network to the internet applies the mask 255.255.255.192 to the destination address of incoming IP packets. If one of the incoming packet has a destination address of 154.33.7.220, then find the network ID, subnet bits and host ID bits of incoming packets respectively
(a) 154.33.7, 11, 011100
(b) 154.33, 11000000, 011100
(c) 154.33, 0000011111, 011100
(d) 154.33.7, 011111, 011100

21. If one of the address of a block is 210.69.92.39/26, then find the last host of the 2nd last subnet, where the addresses are referred in lexicographic order.
(a) 210.69.92.127/26 (b) 210.69.92.192/26
(c) 210.69.92.191/26 (d) 210.69.92.254/26

22. Consider the address: 141.14.196.46 and subnet mask 255.255.192.0. What are the subnet ID and HOST ID.
(a) 141.14.192.0 and 141.14.4.46
(b) 141.14.1.46 and 141.14.192.0
(c) 255.255.192.0 and 255.255.4.46
(d) None of these

23. An organization is assigned a block of 2048 contiguous address starting at address 128.211.160.0 and highest address 128.211.191.255. Which of the following represents the CIDR (Classless Inter Domain Routing)
(a) 128.211.168.0/11 (b) 128.211.160.0/29
(c) 128.211.160.0/19 (d) 128.211.175.255/21

24. There are three IP addresses as given below:
X = 202.23.14.150
Y = 168.19.200.12
Z = 72.192.52.210
Which of the following statements is/are correct?
(a) *X* is Class *A*, *Y* is Class *B* and *Z* is Class *C*
(b) *X* is Class *C*, *Y* is Class A and *Z* is Class *B*
(c) *X* is Class *C*, *Y* is Class B and *Z* is Class *A*
(d) *X* is Class *A*, *Y* is Class C and *Z* is Class *B*

25. In a class *A* subnet, we know the IP address of one of the hosts and the mask as given below:
IP address = 25.34.12.56
Mask = 255.255.0.0
What is the first address (network address)?
(a) 25.34.12.0 (b) 25.34.12.56
(c) 25.34.0.0 (d) 25.0.0.0

26. In a class *B* subnet, we know the IP address of one host and the mask as given below:
IP address = 125.134.112.66
Mask = 255.255.224.0

What is the first address (Network address)?
(a) 125.134.96.0 (b) 125.134.112.0
(c) 125.134.112.66 (d) 125.134.0.0

27. For a class C network if IP address of a computer is 200.99.39.112 and subnet mask is 255.255.255.224 the first host of first subnet (represent last octet) is _____.

28. Which of following IPs may belong to last host of any subnet if subnet mask is 255.255.255.224.
(*i*) 210.15.16.62 (*ii*) 210.15.16.94
(*iii*) 210.15.16.127 (*iv*) 210.15.16.191
(a) (*i*) and (*ii*) (b) (*i*) and (*iii*)
(c) (*ii*) and (*iv*) (d) (*iii*) and (*iv*)

29. A network is determined by the subnet ID 134.96.51.64 and a 26 bit net mask. How many hosts are addressable in the provided network?

30. In a network that has a maximum packet size of 600 bytes, a maximum packet lifetime of 30s, and an 8-bit packet sequence number, what is the maximum data rate (in bps) per connection?

31. A company has class *C* network address of 200.200.200.0. It wishes to have four subnet. Two subnets with 60 hosts one with 20 hosts and with 10 hosts each. Which of the following option respect to a feasible set of subnet address and subnet mask pairs?
(a) 200.200.200.64/255.255.255.192
200.200.200.128/255.255.255.192
200.200.200.32/255.255.255.224
200.200.200.16/255.255.255.240
(b) 200.200.200.128/255.255.255.128
200.200.200.192/255.255.255.128
200.200.200.192/255.255.255.224
200.200.200.240/255.255.255.240
(c) 200.200.200.192/255.255.255.128
200.200.200.128/255.255.255.192
200.200.200.96/255.255.255.112
200.200.200.102/255.255.255.240
(d) 200.200.200.128/255.255.255.128
200.200.200.192/255.255.255.128
200.200.200.64/255.255.255.192
200.200.200.208/255.255.255.208

32. Let *X* and *Y* be the number of 1's in the binary notation of network ID and Direct Broadcast Address (DBA) respectively for the IP address 200.25.80.117 (classfull address). The value of $X^2 + Y^2$ is _____.

33. In the network 251.12.10.110/28, the Fourth octal of max IP address of the network which cannot be assigned to a host is _____.

■■■■

Answers Networking Fundamentals and Physical Layer

1.	(a)	2.	(c)	3.	(c)	4.	(b)	5.	(d)	6.	(d)	7.	(a)	8.	(d)	9.	(d)		
10.	(b)	11.	(b)	12.	(b)	13.	(b)	14.	(b)	15.	(d)	17.	(b)	19.	(d)	20.	(c)		
21.	(c)	22.	(a)	23.	(c)	24.	(c)	25.	(c)	26.	(a)	28.	(a)	31.	(a)				

Explanations Networking Fundamentals and Physical Layer

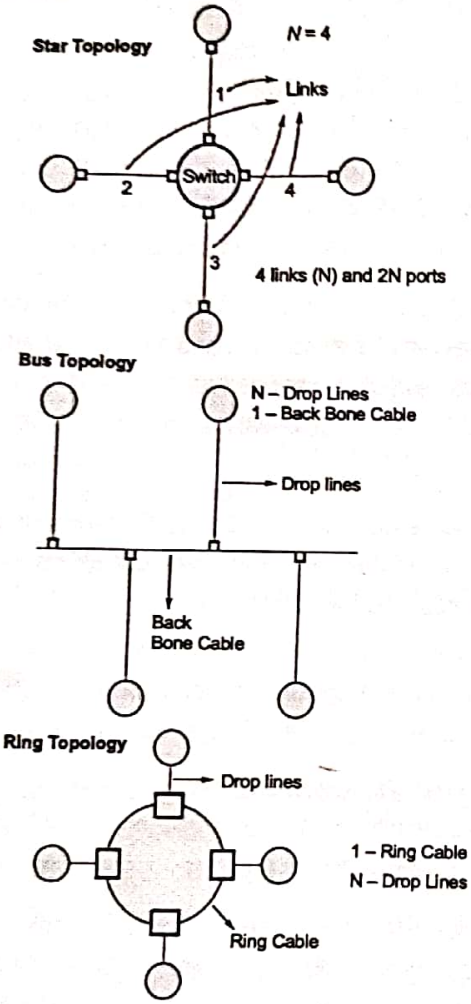
1. **(a)**
Hub works in physical layer
Bridge works in data link layer
Router works in network layer
PC, Server works in application layer.

2. **(c)**
Link layer unit of data is frame
Network layer unit of data is datagram
Application layer unit of data is message
Transport layer unit of data is segment
Note: Network layer can use the term packet if communication is reliable (via TCP).

3. **(c)**
Gateway is used between two dissimilar LAN's, converts a data packet from one protocol format to another protocol format.

4. **(b)**
Every device in the network connects to hub and broadcasts to all devices connected to the hub whenever any transmission received on any port.

6. **(d)**



7. **(a)**
Only gateway can connect to network with different protocols.
Passive device: They do not have any intelligence and they can just forward data.

8. **(d)**
(i) OSI model reduces complexity by breaking network communication into smaller and simpler components. It provides a teaching tool to help network administrators understand the communication process used between networking components.
(ii) OSI model defines the process for connecting two layers together, promoting interoperability between vendors. It allows vendors to compartmentalize their design efforts to fit a modular design, which eases implementations and simplifies troubleshooting.
(iii) OSI model ensures interoperable technology.
(iv) The data link layer protocols often include physical layer specifications. The network and transport layer protocols work together to provide a cummulative end-to-end communication service.
∴ All are true.

9. **(d)**
Option (a): Error Checking is only for header part.
Option (b): There is no acknowledgment for packets reaching the destination.
Option (c): IP has minimal error control and there is no concept of error correction for IP datagram.
All the options are correct.

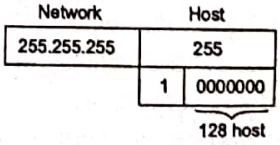
10. **(b)**

$$\text{Efficiency of Ethernet} = \frac{1}{1+6.44a}$$

$$\text{and} \quad a = \frac{\text{Propogation delay } (t_p)}{\text{Transmission delay } (t_t)}$$

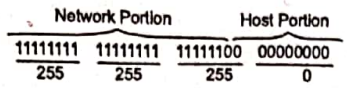
Since a is in denominator its value should be low in order to get high efficiency.

12. **(b)**



Subnet mask is: 255.255.255.128

13. (b)



22-bits are used for network portion
Net mask = 255.255.252.0

14. (b)

Packet A: The source IP contain direct broad cast address and we never use direct broadcast address in source IP. It is always used in destination IP. Hence packet A never exists.

Packet B: If destination IP address contain all 1's then it broadcasts within same network (Limited Broadcasting).

Packet C: It is a unicast packet within the same network as network ID 24.0.0.0 is same for both source and destination IP.

15. (d)

255.255.255.224 provides 0 subnet, each with 30 hosts. So this is useful.

16. (240)

= 1111 0000 [In Binary]

So total No of subjet possible = $2^4 - 2 = 14$. 2 is deducted becuase one for network id and other for broadcast id.

18. (252 & 0)

It is class B IP
So No of host = $2^n - 2 = 600$
So $2^n = 602$, n = 10 [approx]
Hence subnet mask : 255.255.252.0

19. (d)

In 32 bit IP addressing scheme all 1's represent limited broadcast.

20. (c)

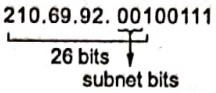
IP Addr: 154.33.7.220
Mask : 255.255.255.192 {apply BITWISE AND}

10011010 . 00010001 . 00000111 . 11000000

220 : 111 011100
Host bits in IP

Destination address is of class B network. Therefore Network ID is 154.33 and as per mask we can say that 10 bits are used for subnetting and remaining are host bits.
∴ Subnet ID bits are 0000011111 and Host ID bits are 011100.

21. (c)



00
01
10 → 2nd Last subnet
11

210.69.92.10 000 000
10 000 001
⋮
210.69.92.10 111 111

⇒ 210.69.92.191

22. (a)

141.14.196.46
141.14.11000100.00101110
Subnet mask 255.255.110000000.00000000
Subnet ID: 141.14.192.0
Host ID: 141.14.4.46

23. (c)

Lowest 128.211.160.0
= 10000000.11010011.10100000.00000000
Highest 128.211.191.255
= 10000000.11010011.10111111.11111111
So here = 32 – 13 = 19

24. (c)

In IP addresses class *A*, *B*, and *C* used for general purpose.
Range of class *A*: 1.0.0.0 to 12.255.255.255
Range of class *B*: 128.0.0.0 to 191.255.255.255
Range of class *C*: 192.0.0.0 to 223.255.255.255
Hence option (c) is correct.

25. (c)

Mask = 11111111.11111111.00000000.00000000
IP Address = 00011001.00100010.00001100.00111000
Taking Bitwise AND = 00011001.00100010.00000000.00000000
i.e. 25.34.0.0.

26. (a)

Subnet Mask = 11111111.11111111.11100000.00000000
IP Address = 01111101.10000110.01110000.01000010
Taking Bitwise AND= 01111101.10000110.01100000.00000000
i.e. 125.134.96.0.

27. (33)

Computer IP 200.99.39.112 (200.99.39.01110000)
Subnet mask +255.255.255.224 (255.255.255.11100000)
200.99.39.96 (200.99.39.01100000) (represent 6th subnet)

But we have to find first subnet with first host that is 200.99.39.00100001 = 200.99.39.**33**

28. (a)

Subnet mask is 255.255.255.224

(*i*) 62 ⇒ 001 11110 ⇒ Last host

(*ii*) 94 ⇒ 010 11110 ⇒ Last host

(*iii*) 127 ⇒ 011 11111 ⇒ Direct broadcast address

(*iv*) 191 ⇒ 101 11111 ⇒ Direct broadcast address

29. (62)

6-bits are used for hosts
$2^6 = 64$ different hosts.
Subnet ID and broadcast address are reserved.
∴ 64 – 2 = 62 hosts are addressable.

30. (40960)

Within a packet lifetime, the maximum number of data packets can be sent is $2^8 = 256$, therefore, the maximum data rate is 256 * 600 * 8/30 = 40960 bps.

31. (a)

First of all we have, 200.200.200.00000000
Initially, we need two subnets with 60 hosts.
1st subnet : 200.200.200.01000000
= 200.200.200.64
2nd subnet : 200.200.200.10000000
= 200.200.200.128

These two subnet with subnet mask 255.255.255.192.
Now we need one subnet with 20 hosts.
200.200.200.00100000 = 200.200.200.32
This subnet with subnet mask 255.255.255.224 one subnet with 10 hosts.
200.200.200.00010000 = 200.200.200.16
Subnet with subnet mask 255.255.255.240.

32. (320)

The IP address 200.25.80.47 belongs to class C network. Therefore network ID is 200.25.80.0 and DBA is 200.25.80.255.
The binary representation contains:
11001000.00001101.01010000.00000000
⇒ 8 1's in network ID
11001000.00001101.01010000.11111111
⇒ 161's is DBA.
∴ $8^2 + 16^2 = 320$

33. (111)

251.12.10.110
Network bits are 28.
So network mask = 255.255.255.240

240 = 1 1 1 1 0 0 0 0
110 = 0 1 1 0 1 1 1 0
Network ID

FIRST IP = 251.12.10.97 assignable
⋮
LAST IP = 251.12.10.110 assignable
LAST MOST IP = 251.12.10.111 DBA
Direct broadcast address of network is not assigned to any host.
So, 111 can't assigned to any host.

■■■■

2 CHAPTER
Data Link Layer

1. Which of the following statement is FALSE?
   (a) In Ethernet, each node's physical address is guaranteed to be globally unique.
   (b) The single parity check can detect any odd number of bit errors in a transmitted codeword.
   (c) In Ethernet, a node wishing to transmit might never be allowed to access the channel.
   (d) None of these

2. Which of the following statement is incorrect?
   (a) A reliable data transfer protocol may send multiple packets without waiting for acknowledgements, rather than operating in a stop and wait manner. This technique is called "Pipelining'.
   (b) A process sends/receives messages to/ from the network through a software interface called a "Socket".
   (c) Because an HTTP server maintains no information about the clients, an HTTP server said to be "Statefull".
   (d) The "Traceroute" can be used to determine the number of hops to a destination and the round trip time for each hop.

3. Find the link utilization in stop and wait protocol if the bandwidth of the line is 2×10^3 bps, round trip time is 40 second and the packet size is 1000 bytes.
   (a) 0 (b) 5
   (c) 10 (d) 15

4. Consider a token bucket with maximum rate R = 20 Mbps. Suppose we want to make sure that the maximum rate can only be sent for atmost 5 seconds at a time, and atmost 150 Mb can be sent over any 10 second window. Compute the required value for the token refresh rate (r) in Mbps.
   (a) 5 (b) 10
   (c) 15 (d) 20

5. Consider a link of length 1000 km with 10^9 bps rate connecting a sender and receiver. Assume a fixed packet length of 1250 bytes and sender always has packets to send. Packets are never lost or corrupted in the connection. What is the necessary window size to achieve 100% utilization for a sliding window protocol? Assume signal propagation is 5 ms per km (approximately).
   (a) 100 (b) 1000
   (c) 110 (d) 1100

6. Given a message "1010001101" and CRC error detecting code uses the polynomial $x^5+x^4+x^2+1$. Find the transmitted message using CRC?
   (a) 101000110101011 (b) 101000110101101
   (c) 101000110101110 (d) 101000110111111

7. Consider a 10^7 bps link that is 400km long, with a queue large enough to hold 2000 packets. Assume that packets arrive at the queue with an average rate of 4000 packets per second and that the average packet length is 2000 bits. Find the traffic intensity?
   (a) 0.2 (b) 0.4
   (c) 0.6 (d) 0.8

8. Assume a hypothetical computer network in which the protocol hierarchy has 10 layer. If the sender sends 200 KB message such that 20% of the network bandwidth is filled with headers. What is the size of the header (in KB)?
   (a) 5 (b) 6
   (c) 10 (d) 15

9. Consider a 1000 mile link of 1 Mbps capacity (error-free). If the link is used by a single sender with a saturated queue sending 1250 byte

frames. Assume signal propagation is 5 μs per mile. [1M = 10^6]

Find the link utilization using sliding window protocol with a window size of 7.

(a) 25% (b) 50%
(c) 75% (d) 100%

10. Suppose that it takes 1 ms to send a packet, and 20 ms one-way propagational delay between sender and receiver. The slinding window size = 4. What is the channel utilization.

(a) 0.190 (b) 0.024
(c) 0.019 (d) 0.097

11. Consider two hosts *A* and *B* connected by link of rate '*r*' bits/sec. The two hosts are separated by '*d*' meters. Signal can propagate on the link for '*p*' meter during a time period of 1 sec. If *A* wants to send a video of s bits to *B*, then what is the end to end delay ignoring any possible processing and queuing delays?

(a) $T_{\text{end to end}} = \dfrac{dr+sp}{pr}$

(b) $T_{\text{end to end}} = \dfrac{dr-sp}{pr}$

(c) $T_{\text{end to end}} = \dfrac{2dr-sp}{pr}$

(d) $T_{\text{end to end}} = \dfrac{dr-2sp}{pr}$

12. Identify the true statements from the following:

I. In STOP and WAIT ARQ if the receiver replies with ACK 0, then the sender will send next frame with sequence number as 1.

II. Physical layer recognizes the frames sent by sender and arranges them in particular order and gives it to layer-2 (Data link layer)

III. ACK sent by receiver also contains CRC.

IV. Stop and wait flow control gives inefficient line utilization for very high data rates over long distance.

V. In sliding window protocol ACK includes the number of next frames to be send.

(a) Only I, IV (b) II, III and IV
(c) III, IV and V (d) I, II, IV, V only

13. Which of the following are true?

I. If maximum window size is *Q*, then number of sequence bits for SR-ARQ and GBN-ARQ are $\log_2(Q+1)$ and $\log_2(2Q)$ respectively.

II. The correct order of buffer sizes in stop and wait, GBN and SR is: (STOP and Wait) < GBN < (selective repeat).

III. GBN and selective repeat supports both individual and cumulative ACK's.

IV. If maximum sequence number is *K*, then maximum sender's window size in GBN and selective repeat are $\dfrac{K+1}{2}$ and $\dfrac{K}{2}$ respectively.

(a) Only II and III (b) Only I and III
(c) Only III and IV (d) None of these

14. What is the total overhead bits (Headers & Retransmission) with data frames consisting of 40 bit header and 3960 data bits. ACK frames never occur. NAK frames are 40 bits ,the error rate (in bits) for frame is 2% and for NAK frame is negligible (upto 2 decimal place)?

15. Imagine a flow specification that has the maximum packet size 800 bytes, token bucket rate of 5×10^6 bytes / sec. Token bucket size is 1 million byte and the maximum transmission rate 10 million bytes / sec. How long can a burst be send at maximum speed?

(a) 0.4 (b) 0.25
(c) 0.2 (d) 0.35

16. Consider GBN protocol in which sender window size (SWS) is 4 and receiver window size (RWS) is 4. Suppose client sends date 0, 1, 2, 3 and only data packet 2 is lost and all ACKs are lost. What will be the contents in the receiver window before sender's timeout value expires?

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

17. Consider two hosts A and B connected by a single link of rate r bits/sec. The two hosts are separated by 'd' meters. Signal propagation is 'p' meters per second. Host A is sending to host B a packet of size 'S' bits. Propagation delay is denoted by 't_{pr}' and transmission delay of packet is 't_{tr}'. Given that, $t_{pr} = \frac{d}{p}$ and $t_{tr} = \frac{S}{r}$.

Which of the following statement is CORRECT?

(a) At time $t = t_{tr}$, the first bit is on the link, if $t_{pr} > t_{tr}$

(b) At time $t = t_{tr}$, the first bit has not reached Host B, if $t_{pr} < t_{tr}$

(c) Both (a) and (b)

(d) Neither (a) nor (b)

18. The message 100100 is to be transmitted by taking the CRC polynomial $x^3 + x^2 + 1$ to protect it from errors. What must be the message to be send after appending the CRC to the message?

(a) 100100000 (b) 100100001

(c) 100100110 (d) 100100111

19. Find the link utilization in stop and wait protocol if the bandwidth of the line is 2×10^3 bps, round trip time is 40 second and the packet size is 1000 bytes.

(a) 0 (b) 5

(c) 10 (d) 15

20. Error detection at the data link layer is achieved by

(a) Bit Stuffing

(b) Hamming codes

(c) Cyclic Redundancy codes

(d) Equalization

21. In CRC if the data unit is 100111001 and the divisor is 1011 then what is dividend at the receiver?

(a) 100111001101 (b) 100111001011

(c) 100111001 (d) 100111001110

22. CRC can detect all bursts of upto m errors, if generator polynomial $G(x)$ is of degree

(a) One (b) $m - 1$

(c) m (d) $m + 1$

23. A 3000 km long trunk is used to transmit frames using a Go-Back-N protocol . The propagation speed is 6msec/km and trunk data rate is 1.544 Mbps. We ignore the time taken to receive the bits in the acknowledgment. Frame size is 64 bytes. If Go-Back-N protocol is used, in order to achieve an efficiency of 100%, what is the maximum window size at the sender's side?

(a) 32 (b) 63

(c) 110 (d) 219

24. A channel has bit rate of 1Mbps and propagation delay of 270 msec. Frame size is of 125 bytes. Acknowledgment is always piggybacked onto data frames. Four bit sequence number is used. Ignore header size. What is the maximum achievable channel utilization for Go Back N?

(a) 1.48% (b) 0.18%

(c) 2.95% (d) 2.78%

25. A channel is operating at 5000bps and the propagation delay is 15 ms. What would be the minimum frame size for stop and wait flow control to get 60% link utilization efficiency?

(a) 225 bits (b) 400 bits

(c) 450 bits (d) 500 bits

26. 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 sender and receiver 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 total time required in this communication?

(a) 250 µsec (b) 200 µsec

(c) 275 µsec (d) 450 µsec

27. The distance between two stations M and N is L kilometers. All frames are K bits long. The propagation delay per kilometer is t seconds. Let R bits/second 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 utilization 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) $\left\lceil \log_2 \frac{2LtR + K}{2K} \right\rceil$

28. To provide more reliability than the Single Parity Bit technique, a new error-detecting scheme has been proposed. The scheme uses first parity bit for checking all the odd numbered bits and a second parity bit for all the even numbered bits. What is the (minimum) Hamming distance of this code?

29. Match **List-I** with **List-II** and select the correct answer using the codes given below the lists:

List-I

A. Stop and Wait ARQ

B. Go-back N ARQ

C. Selective repeat ARQ

List-II

1. Each frame sent or resent needs a timer, which means that the timer needs to be numbered.

2. Ack are sent when data is delivered to network layer. It might be the case that, a single Ack acknowledges *n* frames.

3. Only 2 sequence number used and sender window size is 1.

4. No action performed by the received till the desired frame is obtained.

Codes:

	A	B	C
(a)	3	1	2
(b)	3	2	1
(c)	3	4	1
(d)	2	1	4

30. In selective repeat (*R*) protocol the sender window size is *K* frames. The number of sequence bits required for the communication to take place is given by

(a) $\log_2(K + 1)$

(b) $1 + \log_2(K)$

(c) $1 + \log_2(2K)$

(d) None of these

31. Station *A* needs to send a message consisting of 10 packets to station *B* using a sliding window of size 4. All packets are ready and can be transferred immediately. Selective repeat and GBN are used at 2 different times and every 5^{th} packet get lost for both protocols. (ACK's from B never gets lost). Let x and y be the number of transmissions that *A* has to make in selective repeat and GBN respectively to ensure safe delivery to *B*. Then $x + y =$ _____ ?

■■■■

Answers Data Link Layer

1.	(d)	2.	(c)	3.	(c)	4.	(b)	5.	(b)	6.	(c)	7.	(d)	8.	(a)	9.	(d)
10.	(d)	11.	(a)	12.	(c)	13.	(d)	15.	(c)	16.	(c)	17.	(c)	18.	(b)	19.	(c)
20.	(c)	21.	(b)	22.	(c)	23.	(c)	24.	(d)	25.	(a)	26.	(d)	27.	(c)	29.	(c)
30.	(b)																

Explanations Data Link Layer

1. (d)
Option (a), (b) and (c) are true statements.

2. (c)
Options (a), (b) and (d) are correct statements.
HTTP server maintains no information about clients, such HTTP server is said to be Stateless.
∴ Option (c) is incorrect statement.

3. (c)
Throughput for stop and wait is given by one window per RTT

$$T = \frac{1\text{ packet}}{RTT} = \frac{1000\times 8\text{ bits}}{40\text{ second}} = 200\text{ bps}$$

$$\eta = \frac{200\text{ bps}}{2\times 10^3\text{ bps}}\times 100 = 10\%$$

4. (b)
If we send maximum rate for 5 seconds,
⇒ 20 Mbps × 5 seconds = 100 Mb can be send
Atmost 150 Mb can be sent over any 10 seconds window,
Therefore in remaining 5 seconds:
150 Mb – 100 Mb = 50 Mb can be send

$$\text{Token refresh rate } (r) = \frac{50\text{Mb}}{5\text{sec}} = 10\text{Mbps}$$

5. (b)
To achieve maximum throughput
$U = 1$

$$\therefore \quad = \frac{w.t_{trans}}{t_{trans}+2.t_{prop}} = 1 = 1$$

$$\Rightarrow \quad W = \frac{t_{trans}+2.t_{prop}}{t_{trans}}$$

$$t_{trans} = \frac{1250\times 8\text{ bits}}{10^9\text{bps}} = 0.01\text{ ms},$$

$$t_{prop} = 5\mu\text{ per km} \times 1000 = 5\text{ msec}$$

$$\Rightarrow \quad W = \frac{0.01+2\times 5}{0.01} = \frac{10.01}{0.01} \cong 1000$$

6. (c)

$$M = 1010001101$$

$$P = x^5 + x^4 + x^2 + 1 = 110101$$

```
110101 ) 1010001101 00000 ( 1101010110
         110101
          111011
          110101
           111010
           110101
            111110
            110101
             101100
             110101
              110010
              110101
               01110
```

CRC = 01110
Transmitted message = 101000110101110

7. (d)
Traffic intensity (I)

$$= \frac{\text{Arrival rate (bps)}}{\text{Link bandwidth (bps)}}$$

$$= \frac{4000\text{ packets/sec}\times 2000\text{ bits/packet}}{10^7\text{ bps}} = 0.8$$

8. (a)
Fraction network bandwidth filled with headers

$$= 20\% = \frac{1}{5}$$

$$\text{i.e.} \quad \frac{1}{5} = \frac{10\times \text{header\_size}}{200\text{ kB}+10\times\text{header\_size}}$$

200 kB + 10 × Header_size = 50 × Header_size
200 kB = 40× Header_size
Header_size = 5 kB

9. (d)

If $[(w.t_{trans}) > (2 \times t_{prop} + t_{trans})]$

then $U = 100\ \%$

else $U = \dfrac{w.t_{trans}}{2t_{prop} + t_{trans}}$

$w.t_{trans} = 7 \times 10$ msec $= 70$ msec

$2t_{prop} + t_{trans} = 2 \times (5$ ms$) + 10$ msec $= 20$ msec

$\therefore \quad U = 100\%\ (70 > 20)$

10. (d)

$$\text{Link utilization} = \frac{N}{1+\dfrac{2t_p}{t_t}}$$

Hence $N = 4$

$t_p = 20$ ms

$t_t = 1$ ms

$$\Rightarrow \frac{4}{1+\dfrac{2\times 20}{1}} = \frac{4}{1+40} = \frac{4}{41} = 0.097$$

11. (a)

Since we are ignoring processing and Queueing delays

$$T_{\text{end to end}} = T_{\text{propagation delay}} + T_{\text{transmission delay}}$$

$$= \frac{d}{p} + \frac{s}{r} = \frac{dr + sp}{pr}$$

12. (c)

I is wrong because if frame 0 is sent then receiver will send ACK-1 for requesting frame 1.

II is wrong because physical layer only transmits and receives bits. DLL recognizes the frames.

13. (d)

All the statements are false.

- If max window size is 'Q', then number of sequence bits for GBN ARQ is $\log_2 (Q + 1)$ and for SR ARQ is $\log_2 (2Q)$.
- Stop and wait < selective repeat < GBN is the correct order for buffer sizes.
  As sender's window size is highest in GBN for a particular number of sequence bits.
- GBN supports both individual and cumulative, but SR supports only individual ACK.
- If maximum sequence number is 'K' maximum senders windows size for GBN is $K + 1$ and for selective repeat is $\dfrac{(K+1)}{2}$.

14. (120.80)

The number of retransmissions per frame is 2% i.e., 0.02. Each good frame wastes 40 header bits plus 2% of 4000 bits (retransmission), plus two 40 bit NAK once every 100 frames.

The total overhead $= 40 + 2 \times 40 + 2 \times 0.4$

$= 120.8$ bits.

15. (c)

$$\boxed{t = \frac{C}{M - P}}$$

Where C : Capacity of token bucket

ρ : Token generation rate

M : Maximum data rate of token bucket

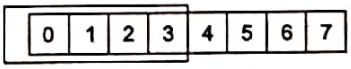
t = time for which token bucket can send the data with maximum data rate.

So, $$t = \frac{1\times 10^6 \text{ bytes}}{10\times 10^6 \text{ bytes/sec.} - 5\times 10^6 \text{ bytes/sec}}$$

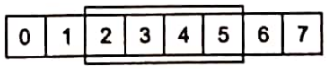
$$t = \frac{1}{5} = 0.2 \text{ sec}$$

16. (c)

Sender window initially :



When 2 is lost then timer expires and window becomes



17. (c)

The first bit is on the link if $t_{pr} > t_{tr}$ and the first bit has reached host B if $t_{pr} < t_{tr}$

18. (b)

- CRC polynomial is the divisor and the message is dividend. The remainder is added to the message and then it is sent.
- CRC is always number of bits in divisor –1.

19. (c)

Throughput for stop and wait is given by one window per RTT

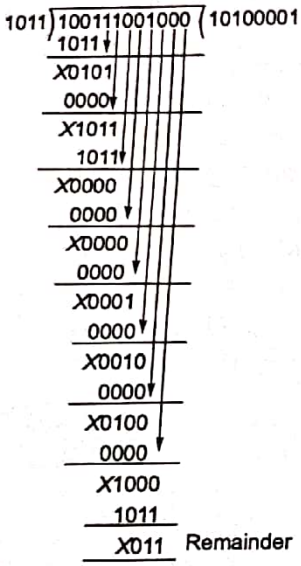
$$T = \frac{1\text{ packet}}{\text{RTT}} = \frac{1000\times 8\text{ bits}}{40\text{ second}} = 200\text{ bps}$$

$$\eta = \frac{200\text{ bps}}{2\times 10^3\text{ bps}}\times 100 = 10\%$$

20. (c)

Error detection at data link layer is achieved by CRC.

21. (b)



So divident at reciver end = 100111001011.

22. (c)

CRC guarantees that all burst error of length equal to the degree of the polynomials are detected and also burst errors affecting an odd number of bits are detected.

23. (c)

For sliding window protocol with Go-Back-N

Data rate = 1.544 Mbps

Frame size = 64 bytes = 64 × 8 bits = 512 bits

Propagation speed = 6×10^{-6} s/km

Distance = 3000 km

Utilization = 100%

$$\Rightarrow \quad U = \frac{W\times T_t}{T_t + 2T_p}$$

$$T_p = 3000 \times 6 \times 10^{-6}\text{ sec}$$

$$T_t = \frac{512\text{ bits}}{1.544\text{ Mbps}}$$

$$= 18\text{ msec} = 0.33\text{ msec}$$

$$\Rightarrow \quad 1 = \frac{W\times 0.33}{0.33 + 2\times 18}$$

$$\Rightarrow \quad W = \frac{36.33}{0.33} \approx 110$$

Window size = 110

24. (d)

Data rate = 1 Mbps

T_p = 270 msec

F = 125 bytes = 125 × 8 bits

= 1000 bits

$$\text{Transmission time } (T_t) = \frac{1000\text{ bits}}{1\text{ Mbps}}$$

$$= 1000 \times 10^{-6}\text{ sec} = 1\text{ ms}$$

Four bit sequence number

For Go-back-N, $W = 16 - 1 = 15$

$$U = \frac{15\times 1}{1+2\times 270}$$

$$= \frac{15}{1+540} = \frac{15}{541} = 0.0277$$

U = 2.78%

25. (a)

For stop and wait

Data rate r = 5000 bps

Propagation delay T_P = 15 msec

Frame size F = ?

U = 60%

$$T_t = \frac{F}{r}$$

$$\Rightarrow \quad 0.6 = \frac{T_t}{T_t + 2T_p} = \frac{1}{1+2\frac{T_p}{T_t}}$$

$$\Rightarrow \quad 0.6 = \frac{1}{1+\frac{2\times 15}{F}\times 5}$$

$$\Rightarrow \quad F = 225\text{ bits}$$

26. (d)

Given, Window size $n = 5$ packets

Packets size = 1000 byte = 2^{10} bits

Total packet size = 5 × 1000 = 5000 bytes

Total time = (Transmission + Propagation) time

= 5 × 50 + 200 μsec = 450 μsec

27. (c)

Frame size K bit long

Propagation delay t sec/km

Channel capacity = R bits/sec

$$U = \frac{W.\frac{K}{R}\text{sec}}{\frac{K}{R}\text{sec} + 2Lt} \qquad 1 = \frac{\frac{WK}{R}\text{sec}}{\frac{K + 2LtR}{R}}$$

$$W = \frac{K + 2LtR}{K} \qquad 2^n = \frac{K + 2LtR}{K}$$

$$n = \left[\log_2 \frac{K + 2LtR}{K}\right]$$

28. (2)

Although the first parity bit can detect odd-numbered bits and the second parity bit can detect even-numbered bits, this coding scheme can only detect ALL single error for sure, that is, $d = 1$. Therefore, the Hamming distance is $d + 1 = 2$. Although it can sometimes detect 2 errors (one even-numbered, one odd-numbered), it cannot detect all the 2 errors.

29. (c)

In **Selective repeat ARQ :** Each frame sent or resent needs a timer, which means that the timer needs to be numbered.

In **Go-back N ARQ :** No action performed by the receiver till the desired frame is obtained.

In **Selective repeat ARQ :** Ack are sent when data is delivered to network layer. It might be the case that, a single Ack acknowledges n frames.

In **Stop and Wait ARQ :** Only 2 sequence number used and sender window size is 1.

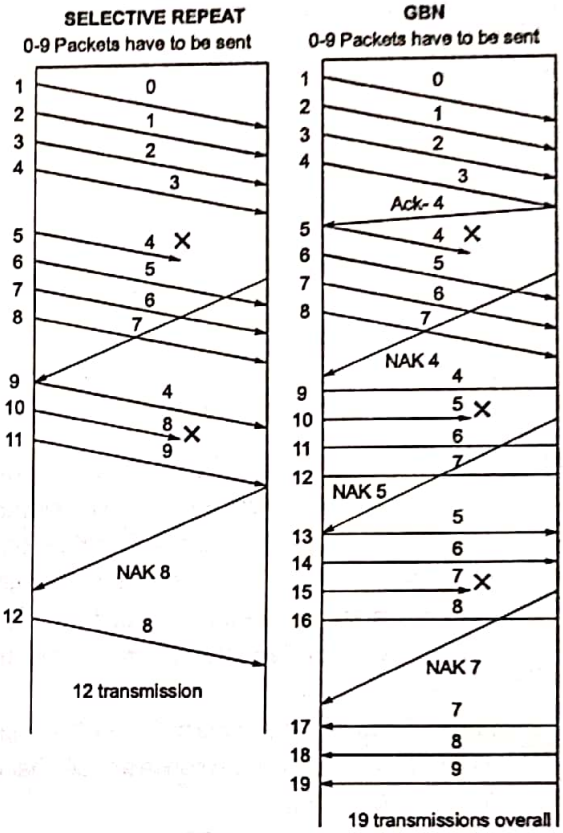
30. (b)

In SR protocol both sender and receiver will have same window size (K in this case).

$\therefore$ Total sequence bits are $\log_2(K + K) = \log_2(2K) = \log_2 2 + \log_2 K = 1 + \log_2 K$.

31. (31)

In R.T.T time, only 4 (window size) frames can be transmitted in sliding window protocol.



$x = 12$

$y = 19$

$\Rightarrow \quad x + y = 31$

■■■■

3 CHAPTER

MAC Sub-Layer

1. Match List-I (Device) with List-II (Operating Layer) and select the correct answer using the codes given below the lists:

List-I	List-II
A. Repeater	1. Physical layer
B. Bridge	2. Datalink layer
C. Gateway	3. Network layer
D. Router	4. All layers

Codes

	A	B	C	D
(a)	1	2	3	4
(b)	2	4	1	3
(c)	1	2	4	3
(d)	2	3	1	4

2. Consider two nodes A and B on the same ethernet segment, and suppose the propagation delay between the two nodes is 225 bit times. Suppose at time both nodes A and B begin to transmit a frame. Assume that both nodes transmit a 50-bit jam signal after detecting a collision.
For 10^7 bits per set ethernet, find the time at which both nodes A and B sense an idle channel? [in micro seconds]]
(a) 22 μs (b) 27 μs
(c) 50 μs (d) 55 μs

3. In P-persistent CSMA network there are 5 systems in a slot. The probability of station not transmitting the data is 0.6. Only two stations should transmit the data to avoid collision. What is the probability that channel is collision free?

4. Consider nodes in slotted-aloha transmit in each slot with probability $P = 0.25$. Suppose that a given channel has exactly 8 nodes. What is the probability there is a collision in a given slot _____? [upto three decimal]

5. Consider a 1 Mbps ethernet and find the throughput for slotted aloha at $G = 2$ (channel load) in Kbps.

6. In shared ethernet link, each user is active only 10% of the time. Suppose packet switching is used for 10 users and each user is equally likely to transmit at any point of time. The probability p that at any given time exactly 8 users are transmitting simultaneously. What is the value of $10^{10} \times p$?

7. In synchronous transmission, 5 eight bit characters are included in 30 eight bit information characters. If bit rate of sender is 4200 bits/sec, what is the bit rate of receiver (in bits per sec)?

8. Which of the following are true?
I. In ethernet, if the node transmission rate is increased while all other parameters are held constant then throughput increases.
II. The IEEE 802.2 LLC protocol is specific to the technology being used in a particular broadcast LAN, and therefore must be defined separately for ethernet, token ring, etc.
III. Bandwidth is the maximum throughput of the channel.
(a) Only I and III
(b) All of I, II, and III
(c) Only III
(d) All are False

9. Suppose that 2 N ethernet stations are trying to send the frame, at the same time requires $N/2$ slot time to sort out, who will transmit next. Assume that the average packet transmission time is 10 slots. Express the utilization of ethernet in terms of N.

(a) $\frac{10}{10+2N}$ (b) $\frac{20}{30+2N}$

(c) $\frac{20}{20+N}$ (d) $\frac{20+N}{10}$

10. For a standard Ethernet bandwidth is 10 Mbps the minimum frame size should be 64 bytes. To support CSMA/CD, Transmission Time is twice of Propagation Delay. In fast Ethernet, what will be the length of cable to support same frame size of 64 bytes, if L is length of cable in standard Ethernet?
(a) $10L$ (b) $5L$
(c) $L/10$ (d) $L/5$

11. Which of the following statement is false to deploy a router?
(a) The LANs interconnected must belong to different networks.
(b) The Ethernet interface and the LAN must belong to the same network.
(c) The Routers sharing the same link must belong to the same network.
(d) All the interfaces of the router must belong to same network.

12. If the data rate of ring is 20 Mbps, signal propagation speed is 200 b/μs, then the number of bits that can be placed on the channel of 200 km is
(a) 2,000 bits (b) 20,000 bits
(c) 1,000 bits (d) none of these

13. A group of N stations share 50 Kbps slotted ALOHA channel. Each station outputs a 500bits frame on an average of once 5000 ms, even if previous one has not been sent. What is the maximum value of N?
(a) 184 stations (b) 368 stations
(c) 412 stations (d) 450 stations

14. CSMA/CD LAN of 1 Gpbs is to be designed over 100 m cable without repeater. What is the minimum frame size that Data Linked Layer should consider if cable support signal speed of 200000 Km/sec?

15. A group of some stations share a 56 kbps pure ALOHA channel. Each of these stations output a 1000 bits frame on an average of one every 100 seconds, even if the previous one not yet been sent. Efficiency of pure ALOHA is 18.4%. What would be the maximum number of stations?

16. To support CSMA /CD Transmission Time is equal to double the propagation time. What is the length of cable (in meters) used in fast Ethernet if bandwidth = 100×10^6 bps, frame size = 64 bytes velocity = 2×10^8 m/sec to support CSMA / CD

■■■■

Answers MAC Sub-Layer

1. (c) 2. (c) 8. (a) 9. (c) 10. (c) 11. (d) 12. (b) 13. (a)

Explanations MAC Sub-Layer

1. **(c)**
Repeater – Physical layer
Bridge – Data link layer
Gateway – All layers
Router – Network layer

2. **(c)**
Step 1: Both nodes detect a collision at time $t = 225$.
Step 2: Jam signal has 50-bit
Both nodes stop transmits their jam signal at the time $t = 225 + 50 = 275$
Step 3: The last bit of the jam signal from B arrives at A after 225 bit times, so $275 + 225 = 500$.
(Similarly, the last bit of the jam signal from A arrives at B after 225 bit times, so $275 + 225 = 500$ bit times).
At 500 bit times, both sense an idle channel.
For 10^7 bps ethenet, the time taken for 500 bits:

$$= \frac{500 \text{ bits}}{10^7 \text{ bits/sec}} = 50 \text{ μsec}$$

3. **(0.3456)**

P(of 2 stations)

$$= 5C_2 \times P_{(\text{transmitting})}{}^2 \times P_{(\text{not transmitting})}{}^3$$
$$= 5C_2 (0.4)^2 (0.6)^3$$
$$= 10 \times 0.16 \times 0.216 = 0.3456$$

4. **(0.632)**

A collision occours with probability 1 unless either the channel is used successfully or nobody sends.

So $1 - 8P(1-P)^7 - (1-P)^8$

$$= 1 - 8 \times \frac{1}{4}\left(1-\frac{1}{4}\right)^7 - \left(1-\frac{1}{4}\right)^8$$
$$= 1 - 2\left(\frac{3}{4}\right)^7 - \left(\frac{3}{4}\right)^8$$
$$= 1 - \left(\frac{3}{4}\right)^7\left(2+\frac{3}{4}\right)$$
$$= 1 - \left(\frac{3}{4}\right)^7\left(\frac{11}{4}\right)$$
$$= 1 - \frac{3^7 \times 11}{4^8} = 1(0.367) = 0.362$$

5. **(270)**

Throughput for slotted Aloha at $G = 2$

$$S = Ge^{-G}$$
$$= 2e^{-2} = \frac{2}{e^2} = 0.27 \times 100 = 27\%$$
$$\therefore \quad \frac{27}{100} \times 1\text{Mbps} = 270 \text{ Kbps}$$

6. **(3645)**

$$p_{\text{active}}(8) = {}^{10}C_8 (0.1)^8 (0.9)^{10-8}$$
$$= 45 \times (0.1)^8 \times (9)^2 = 36.45 \times 10^{-8}$$
$$= 0.0000003645 \times 10^{10} = 3645$$

7. **(3500)**

Synchronous bits are not taken by receiver. They are sent by sender just to alert the receiver about the incoming data.

5 eight bit character = 40 bits

30 eight bit character information = 240 bits

40 synchronous bits → 240 info bits

X Synchronous bits → 4200 info bits

$$X = \frac{40 \times 4200}{240} = 700 \text{ synchronous bits}$$

Total data bits = 4200 – 700 = 3500 bits/sec

8. **(a)**

I. $$\text{Throughput} = \frac{\text{Data size}}{T_d + 2 \times pd}$$
$$= \frac{\text{Data size}}{\frac{\text{Data size}}{\text{Bandwidth}} + 2 \times pd}$$
$$= \frac{\text{Bandwidth} \times \text{Data size}}{\text{Data size} + 2 \times \text{bandwidth} \times pd}$$

Keeping everything constant, if bandwidth increases then throughput increases.

II. LLC protocol is not specific to the technology being used.

III. Bandwidth is the maximum number of bits which can be transmitted through the channel under ideal conditions.

9. **(c)**

Let slot time = t

then frame transmission time = $10t$

$$\text{contention period} = \frac{N}{2} \times t$$

$$\text{Utilization } (U) = \frac{10t}{10t + \frac{N}{2}t} = \frac{10}{10 + \frac{1}{2}N} = \frac{20}{20+N}$$

10. **(c)**

Transmission Time = 2 × Propagation Time

$$\frac{\text{Data size}}{\text{B.W.}} = 2 \times \frac{d}{v}$$

Velocity is same when media is same, bandwidth for fast ethernet is 100 Mbps.

In order to maintain the same frame size since bandwidth is increased from 10 to 100 Mbps the distance will be reduced from L to $L/10$.

11. (d)

Option (a), (b), (c) are true

All the interfaces of the router must belong to different network.

Note: The above given statements are rules to deploy a router.

12. (b)

Given, Data Rate = 20 Mbps

Propagation speed

T_P = 200 m/μ sec = 200×10^6 m/sec

$$\text{Time to travel 200 km} = \frac{200\times10^3 \text{ m}}{200\times10^6 \text{ m/s}}$$

$$= 10^{-3} \text{ sec.}$$

Data in 10^{-3} sec = $10^{-3} \times 20$ Mbps

$= 10^{-3} \times 20 \times 10^6 = 20 \times 10^3$

Number of bits = 20,000 bits.

13. (a)

Throughput of one station

$$= \frac{500 \text{ bits}}{5000 \times 10^{-3} \text{ sec}} = 100 \text{ bps}$$

Maximum throughput in case of slotted ALOHA

$$= 50 \times \frac{1}{e} = 50 \times 0.37 = 18.5 \text{ Kbps}$$

So, $N \times$ throughput of one station = maximum throughput

$N \times 100$ bps = 18.5 kbps

$$N = \frac{1.85 \times 10^{-3}}{100} = 185 \approx 184$$

14. (1000)

Data rate = 10^9 bps

Cable length = 100 m

Signal length = 200000 Km/sec

= 2×10^8 m/sec

For CSMA/CD ethernet LAN,

$$t_f \geq 2\, t_p$$

Signal in 1 sec travels 2×10^8 m

$$\text{Frame Length} = \frac{2\times100\text{m}\times10^9 \text{ bps}}{2\times10^8 \text{ m/s}}$$

10^3 = 1000 bits

15. (1030)

$$\text{No. of output bits/sec} = \frac{1000}{100} = 10 \text{ bits/sec}$$

Thus each station outputs 10 bits/sec. If we have N stations, then total number of bits transmitted by all N stations in one second would be 10 N bits.

Usable bandwidth = Efficiency × Data rate

= 18.4% × 56 kbps

= 10.3 kbps

$\because$ Efficiency of pure ALOHA is 18.4%

$\therefore$ $10N = 10300$

$N = 1030$

16. (512)

Transmission Time = 2 × Propagation Time

$$\frac{\text{Frame size}}{\text{B.W.}} = 2\times\frac{d}{v}$$

$$\frac{64\times8 \text{ bits}}{10^8 \text{ bits/sec}} = 2\times\frac{x}{2\times10^8 \text{ m/sec}}$$

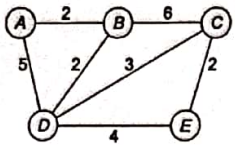
$\Rightarrow$ $512 \text{ m} = x$

■■■■

4 CHAPTER

Network Layer

1. Consider the following subnet:



Find the link state routing table for node *A* using OSPF.

(a)

	Cost	via
A	0	A
B	2	B
C	8	B
D	5	D
E	8	B

(b)

	Cost	via
A	0	A
B	2	B
C	7	D
D	4	B
E	8	B

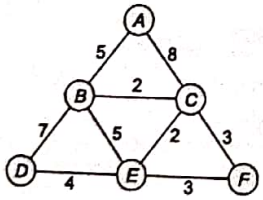
(c)

	Cost	via
A	0	A
B	2	B
C	5	B
D	4	B
E	8	D

(d)

	Cost	via
A	0	A
B	2	B
C	7	B
D	4	B
E	8	B

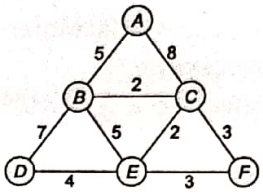
2. Consider the network shown in the following graph with nodes and links along with costs.



Which one of the following link change [remaining will be same], never change the routes of destinations stored at node *B* routing table? (Link change is always ≥ 0)

(a) (*A*, *C*) increase
(b) (*A*, *C*) decrease
(c) (*B*, *C*) increase
(d) (*B*, *C*) decrease

3. Consider the network shown in the following graph with nodes and links along with costs.



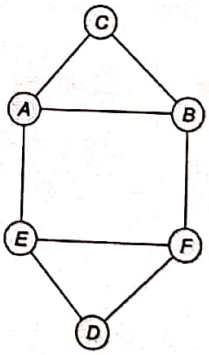
Initially node B's routing table contains only one entry, for itself. When *B* runs dijkstra's algorithm, which of the following is not a correct order of nodes added to the routing table?

(a) *B*, *C*, *E*, *A*, *F*, *D*
(b) *B*, *C*, *E*, *D*, *A*, *F*
(c) *B*, *C*, *E*, *F*, *A*, *D*
(d) None of these

4. A computer on a 6 Mbps network is regulated by a token bucket. The token bucket is filled with a rate of 1Mbps. The bucket is initially filled to capacity with 1Mb. How long can the computer transmit at the full 6 Mbps?

(a) 0 sec
(b) 0.1 sec
(c) 0.2 sec
(d) 0.15 sec

5. The subnet with 6 routers with delays shown as lines in the following graph.



It uses distance vector routing to build the routing tables. Router *A* has measured its routes to its neighbours *B*, *C*, and E. It gets new distance of 2, 1, 5 for *B*, *C*, *E* respectively. *A* has received the following vectors from node *B*: (2, 0, 2, 6, 6, 5), from node *C*: (1, 4, 0, 9, 7, 7), and from node *E*: (6, 8, 7, 5, 0, 3). Find which of the following is the new routing table at *A*.

(a)

To	next hop	distance
A	–	0
B	B	2
C	C	1
D	E	6
E	E	5
F	B	5

(b)

To	next hop	distance
A	–	0
B	B	2
C	C	1
D	E	6
E	E	5
F	B	7

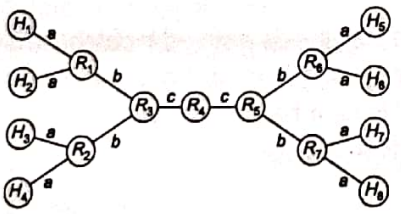
(c)

To	next hop	distance
A	–	0
B	B	2
C	C	1
D	B	5
E	E	5
F	B	7

(d)

To	next hop	distance
A	–	0
B	B	2
C	C	1
D	B	8
E	E	5
F	B	7

6. Consider the network shown below which has eight hosts H_1 to H_8 an seven routers R_1 to R_7 each of which is much faster than any of the links.



All links are shown as a, b and c. All links are full duplex and bandwidth of a is 1Mbps, b is 2Mbps and c is 4Mbps.

Find the routers which can never be congested?

(a) Only R_1, R_2 (b) Only R_6, R_7

(c) Only R_3, R_5 (d) Only R_4

7. Which of the following statements about Link State Protocol (LSP) is/are true?

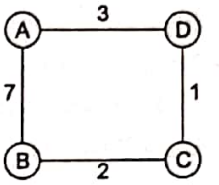
S_1: If LSP data is less recent than the data stored in database, then the new LSP packet is updated with data stored in database and is flooded to channels.

S_2: If LSP data is not in database, then data is stored and LSP packet is forwarded over all interfaces but not to the one on which it was received.

(a) Only S_1 (b) Only S_2

(c) Both S_1 and S_2 (d) Neither of them

8. Consider the network shown below:



The nodes in the network run the distance vector routing algorithm. Which of the following computed as the final distance vectors at node D after all updates are exchanged among routers? Assume that the nodes only know their distances to their direct neighbours initially.

(a) from

to	A	B	C	D
A	0	6	4	3
C	4	2	0	1
D	3	3	1	0

(b) from

to	A	B	C	D
A	0	7	4	3
C	4	2	0	1
D	3	10	1	0

(c) from

to	A	B	C	D
A	0	6	4	3
C	4	2	0	1
D	3	10	1	0

(d) None of these

9. The main characteristic of routing algorithm is the following.

(a) The algorithm should produce results in a stable manner in varying traffic conditions.

(b) The algorithm must be fair in selecting routes.

(c) The algorithm must be able to cope with changes in topology.

(d) All of the above

■■■■

Answers Network Layer

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

Explanations Network Layer

1. (d)

Using optimal shortest path

A to $A = 0$

A to $B = 2$ (via B)

A to $C = 7$ (via B) $A - B - D - C$

A to $D = 4$ (via B) $A - B - D$

A to $E = 8$ (via B) $A - B - D - E$

2. (a)

- If (A, C) link cost increases, it will never effect any route from B. Because (A, C) link with cost 8 is neglected while computing shortest paths from B.
- If (A, C) decreases then it may be used (if cost ≤ 3)
- If (B, C) increases then other routes may effect if cost > 5 then (B, E) link is used insted of $B \rightarrow C \rightarrow E$ path.
- If (B, C) decreases then path B to D may be changed. If (B, C) cost = 0 then $B \rightarrow C \rightarrow E \rightarrow D$ is used instead of $B \rightarrow D$.

3. (b)

B to A link cost is 5 [shortest]

B to F link cost is 5 [shortest]

After B, C, E visits, next node is either A or F but B to D link cost is 7 [shortest] B, C, E, A, F, D.

OR

B, C, E, F, A, D

$\therefore$ Option (b) cannot be the order of nodes added to the routing table at B.

4. (c)

Net outflow from the token bucket is:

$= 6\text{Mbps} - 1\text{Mbps}$

As a result the time it takes for the full bucket of 1 Mb to empty is: 1 Mb / 5 Mbps = 0.2 sec

$\therefore$ During first 0.2 sec, it transmits with 6 Mbps, then switches to 1 Mbps.

5. (d)

	A	B	C	E
A	0	2	1	6
B	2	0	4	8
C	1	2	0	7
D	–	6	9	5
E	5	6	7	0
F	–	5	7	3

$\Rightarrow$

B+2 via B	C+1 via C	E+5 via E
4	2	11
(2)	5	13
4	(1)	12
(8)	10	10
8	8	(5)
(7)	8	8

	Next hoop	Distance
A	–	0
B	B	2
C	C	1
D	B	8
E	E	5
F	B	7

6. (d)

$R4$ can never be congested.

Worst case, all 4 hosts H_1 to H_4 sends to either of H_5 to H_8 or vice-versa.

In this case there is enough link capacity on both sides. But all other can become congested.

7. (b)

S_1 is wrong because, if LSP is with less recent data than the data stored in database is received, then new LSP is updated with database data and is sent back only over the link from which the first LSP was received.

8. (a)

from

to	A	B	C	D
A	0	6	4	3
C	4	2	0	1
D	3	3	1	0

9. (d)

Routing algorithm

(*i*) Produce results in a stable manner in varying traffic conditions.

(*ii*) It is fair in selecting routes for communication.

(*iii*) The changes in the topology are well adjudged.

Hence, (d) is correct option.

■■■■

5 CHAPTER
Transport Layer

1. Which of the following functionality must be implemented by transport layer above network layer?
   (a) Recovery from packet loses
   (b) Detection of duplicate packets
   (c) Packet delivery in correct order
   (d) End to end delivery

2. Consider a TCP connection using the slow start congestion control scheme with an initial threshold value of 64 kB and a Maximum Segment Size (MSS) of 2 kB. The receiver's advertised window is initially 32 kB. The first transmission attempt is numbered 0, and all transmission attempts are successful except for the timeouts on attempt number 4. Find the size (in kB) of the sender's congestion window at attempt number 9.
   (a) 16 (b) 18
   (c) 20 (d) 22

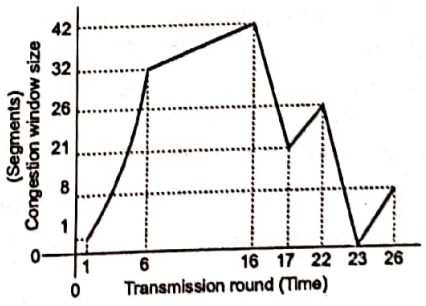
3. ICMP has error reporting messages. Which of the following error reporting message describes the given statement '*S*'?
   S: The packet is discarded due to the processing problem observing a change in the header format of the IP datagram.
   (a) Destination unreachable
   (b) Source quench
   (c) Parameter problem
   (d) Redirection

4. Assume that a new TCP connection starts by sending 1 segment, and then increases it congestion window by 1 segment each time it receives an acknowledgment i.e., after 1 RTT congestion window is 2 segments in slow start. Assume connection never leaves slow start. Find the number of RTT's it takes to send *N* segments.
   (a) $N+1$ (b) $\log_2(N+1)$
   (c) 2^{N+1} (d) $2^{(N+1)}$

5. Suppose that there is a new version of TCP header that accomodates a Round Trip Time (RTT) of 200 ms, a network bandwidth of 10 Mbps. Assume maximum segment life time is 150 seconds. Find the number of bits needed for sequence number field?
   (a) 30 bits (b) 31 bits
   (c) 32 bits (d) 33 bits

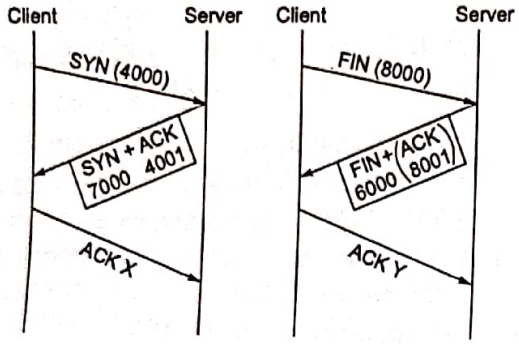
6. Assume that TCP allows window sizes much larger than 64 KB. Suppose this extended TCP over 1 Gbps link with round trip latency (RTT) of 100 msec to transfer a 10 MB file. If TCP sends 1 KB packets by assuming no congestion and no packet loss, find how may RTT's does it take to send the file.
   (a) 10 RTT's (b) 14 RTT's
   (c) 18 RTT's (d) 22 RTT's

7. Consider the following plot of TCP window size as a function of time. Assume TCP is operating with slow start, congestion avoidance, fast retransmit and fast recovery mechanism.



Identity the interval of the time when TCP congestion avoidance is operating [first time].
(a) (1, 6) (b) (6, 16)
(c) (16, 17) (d) (22, 23)

8. Consider the following TCP connection where only control segments are exchanged. The TCP follows the same 3-way handshaking procedure as in circuit switching. FIN and SYN have the usual meaning of TCP connections. What are the possible values of X and Y respectively?



(a) 4002, 8002 (b) 4001, 8001
(c) 7000, 6000 (d) 7001, 6001

9. TCP is sending data at 1 Mbytes/s. If the sequence number with 7000, how long does it take before the sequence number goes back to zero _____ seconds?

10. Assume the TCP round trip time RTT is currently 30 m sec and the following ACK's come in after 26, 32 and 24 ms respectively. What is the new RTT estimate (in ms) using Jacobson's algorithm ($\alpha = 0.9$)? (where α is smoothing factor)

11. Suppose that Host *A* sends over a TCP connection to Host *B* one segment with sequence number 44 and 2 bytes of data. What will be acknowledgment number for the subsequent segment?
(a) 22 (b) 44
(c) 46 (d) 88

12. Consider the following statements regarding TCP's congestion control phases.
(i) The size of the congestion window increases exponentially until it reaches a threshold (in slow start algorithm).
(ii) In multiplicative decrease procedure, threshold gets decreased to one-half of the previous window size.
(iii) The size of the congestion window increases exponentially after achieving threshold value till the timeouts.
Which of the following ever statements are true?
(a) (i), (ii) only (b) (i), (iii) only
(c) (ii), (iii) only (d) (i), (ii) and (iii)

13. To prevent silly window syndrome created by a sender that is sending data at a very slow rate _____ can be used.
(a) Clark's solution
(b) Nagle's algorithm
(c) Both (a) and (b)
(d) Delayed acknowledgement

14. Assume that the main web page (index.html) is a HTML file of size 350,000 bytes and the MSS is 1400 bytes. Further assume that the sequence number for the very first TCP segment carrying that data stream is 0. How many TCP segments are needed in total to transmit that HTML page? Assume there are no packet losses and timeouts.

15. Suppose that the TCP congestion window is set to 18 KB and a time-out occurs. How big (in KB) will the window be if the next four transmission bursts are all successful? Assume that the maximum segment size is 1 KB.

■■■■

Answers Transport Layer

1. (d) 2. (b) 3. (c) 4. (b) 5. (b) 6. (b) 7. (b) 8. (d) 11. (c)
12. (a) 13. (b)

Explanations Transport Layer

2. (b)

Attempt	Sender's Congestion Window (kB)	Threshold (kB)
0	2	64
1	4	64
2	8	64
3	16	64
4	32	64
5	2	16
6	4	16
7	8	16
8	16	16
9	18	16
10	20	16

During attempt number 9, senders congestion window size = 18

3. (c)

- In redirection packet is not discarded but it is redirected to a network as the host doesn't belong to this network.
- In source quench packet is discarded due to congestion in the network.
- Destination unreachable means host is not present in the network or the host is not responding to the request, then the packet is discarded.

4. (b)

Window size [WS = 1] initially
After 1 RTT, WS = 2, #segments sent = 1
After 2 RTT's, WS = 4, #segments sent = 3 (total)
After 3 RTT's, WS = 8, #segments sent = 7 (total)
After 4 RTT's, WS = 16, #segments sent = 15 (total)
⋮
x RTT's $\Rightarrow$ #segments sent $= 2^x - 1 = N$
$2^x - 1 = N \Rightarrow x = \log_2(N+1)$

5. (b)

In 150 seconds, the source can transmit upto 150sec × 10Mbps = 1.875 Gbytes [$<2^{31}$ bytes]
$\therefore$ Number of bits required for sequence number $= \log_2 1.875\ G = 31$ bits

6. (b)

File size = 10MB
Starting window sieze (WS) = 1 KB
After 1 RTT's $\Rightarrow$ WS = 2 KB and transmitted 1 KB
After 2 RTT's $\Rightarrow$ WS = 4 KB and transmitted 3 KB
After 3 RTT's $\Rightarrow$ WS = 8 KB and transmitted 7 KB
After 10 RTT's $\Rightarrow$ WS = 1 MB and transmitted nearly 1 MB
After 11 RTT's $\Rightarrow$ WS = 2 MB and transmitted nearly 2 MB
After 12 RTT's $\Rightarrow$ WS = 4 MB and transmitted nearly 4 MB
After 13 RTT's $\Rightarrow$ WS = 8 MB and transmitted nearly 8 MB
After 14 RTT's $\Rightarrow$ 10 MB file transmitted completely.

7. (b)

Slow start operating interval: (1, 6)
Then congestion avoidance begins.
Congestion avoidance interval: (6, 16)

8. (d)

The respective values are 7001, 6001.
As these are only control segments, no data is shared. Only 1 sequence number is consumed.
Hence 7001, 6001 is correct answer.

9. (4295)

The largest number in the sequence number field is $2^{32} - 1$.
If we start at 7000, it takes $[(2^{32} - 1) - 7000] / 1{,}000{,}000 = 4295$ sec.

10. (29.25)

Smoothed Round trip time proposed by Jacobson's is given as

$$ERTT = \alpha\, IRTT + (1-\alpha)\, NRTT$$

Where, ERTT is estimated RTT.

IRTT is initial RTT.

NRTT is new RTT, α is the smoothly factor.

When ACK comes after 26 ms

$$ERTT = (0.9)\,30 + (0.1)\,26 = 29.6 \text{ ms}$$

When 2nd ACK comes after 32 ms

$$ERRT = \alpha\,(29.6) + (1-\alpha)\,32 = 29.84 \text{ ms}$$

When 3rd ACK comes after 24 sec

$$ERTT = \alpha\,(29.84) + (1-\alpha)\,24 = 29.256 \text{ ms}$$

11. (c)

Segment sequence number = 44

and data = 2 byte

So 44 + 2 = 46 will be the sequence

Number of next byte the receiver is expecting.

12. (a)

In the slow start alogrithm, the size of the congestion window increases exponetially until it reaches a threshold, after this there is additive increases (one-one window) till the time outs.

Statement (iii) is false.

13. (b)

Nagle's algo is used to prevent silly window syndrome created by a sender that send data at a very slow rate.

14. (250)

$$\frac{350000 \text{ bytes}}{1400 \text{ bytes}} = 250 \text{ segments}$$

15. (8)

When a time-out occurs, three things happens. First, slow start will be initiated. Second, the congestion window would start at 1. Third, the threshold will be reset to 18 KB/2 = 9 KB. If the next four transmissions are all successful, then

- 1st transmission : 1 segment, 1 KB
- 2nd transmission : 2 segments, 2 KB
- 3rd transmission : 4 segments, 4 KB
- 4th transmission : 8 segments, 8 KB

After these four successful transmissions, the window size is supposed to be 16. However, since the threshold is 9KB, the window size can only be 9 KB.

■■■■

6 CHAPTER

Application Layer

1. Which of the following is true about Flow Control in FTP and TFTP respectively? (yes, if it exists and no, if does not exist).
   (a) YES, YES (b) NO, NO
   (c) YES, NO (d) NO, YES

2. Which of the following protocol allows non-ASCII data to be sent through e-mail?
   (a) POP3 (b) IMAP4
   (c) TELNET (d) MIME

3. Match **List-I** (Protocol Layers) with **List-II** (Type of address used) and select the correct answer using the codes given below the lists:

List-I	List-II
A. Application layer	1. IP address
B. Network Layer	2. Port address
C. Data link layer	3. MAC address

Codes:

	A	B	C
(a)	1	2	3
(b)	2	3	1
(c)	2	1	3
(d)	3	1	2

4. Match column A with column B

Column A	Column B
1. DNS	(i) Port-20
2. POP3	(ii) Port-21
3. FTP (Data)	(iii) Port-53
4. FTP (Control)	(iv) Port-110
	(v) Port-69

Codes:
(a) 1 - (iii), 2 - (iv), 3 - (ii), 4 - (i)
(b) 1 - (iii), 2 - (iv), 3 - (i), 4 - (ii)
(c) 1 - (iii), 2 - (v), 3- (i), 4 - (ii)
(d) 1 - (iii), 2 - (v), 3 - (ii), 4 - (i)

5. Which is the correct option for statement *P* and *Q*.
   P : Port 80 is used by FTP to transfer data.
   Q : DNS runs on top of UDP.
   (a) Both are true (b) Both are false
   (c) Only *P* is true (d) Only *Q* is true

6. The values in the HTTP message's cookie field stored at the
   (a) Client side (b) Senser side
   (c) Both side (d) None side

7. Match **List-I** with **List-II** and select the correct answer using the codes given below the lists:

List-I
A. HTTP
B. POP
C. SMTP
D. MIME

List-II
1. Sending email messages
2. Transfer Multimedia information
3. Send email attachment
4. Receiving email messages

Codes:

	A	B	C	D
(a)	1	2	3	4
(b)	2	4	1	3
(c)	2	1	4	3
(d)	4	2	3	1

8. You want to implement a mechanics that automates the IP configuration, including IP address, subnet mask, default gateway, and DNS information. Which protocol will you use to accomplish this?
   (a) SMTP (b) SNMP
   (c) DHCP (d) ARP

9. Which of the following services use UDP?
   1. DHCP 2. SMTP
   3. SNMP 4. FTP
   5. HTTP 6. TFTP
   (a) 1, 3 and 6 (b) 2 and 4
   (c) 1, 2 and 4 (d) all of these

10. To convert the "iitb.cse.in" to its IP address, which of the following is needed?
(a) TCP (b) ARP
(c) DNS (d) HTTP

11. Consider the following statements:
1. A user request a webpage, that consists of some text and one image. For this page client will send one request message and receive 4 response messages.
2. Two distinct webpages (for eg. www.madeeasy.in/student.html and ww.madeeasy.in/course.html) can not be sent over the same persistent connection.

Which of the following is correct:
(a) Only 1 is true
(b) Only 2 is false
(c) Both 1 and 2 are true
(d) Both 1 and 2 are false

Answers Application Layer

1. (d) 2. (d) 3. (c) 4. (b) 5. (d) 6. (c) 7. (b) 8. (c) 9. (a)
10. (c) 11. (d)

Explanations Application Layer

1. **(d)**
- FTP does not have flow control and has to depend on other protocol (TCP).
- In TFTP flow control exists, therefore it does not depend on other protocols. Hence it uses UDP as transport layer protocol.

2. **(d)**
Multipurpose internet mail extension is a supplementary protocol that allows non-ASCII data to be sent through e-mail.

3. **(c)**
Application layer uses port numbers (address). Network layer deals with IP addresses and Data link layer deals with physical address of the device (MAC address).

4. **(b)**
DNS port number is 53, POP3 uses port number 110, FTP uses 2 ports : First port for data communication: 20, for connection estabilshment: 21.

5. **(d)**
FTP uses port 20 to transfer data so statement *P* is false and *Q* is correct statement.

6. **(c)**
A cookie can be used to maintain state between HTTP transaction. So both client and server store the cookie value.

7. **(b)**
HTTP: Transfer Multimedia Information
POP: Receiving email messages
SMTP: Sending email messages
MIME: Send email attachments
HTTP: Hyper text transfer protocol
POP: Post office protocol
SMTP: Simple mail transfer protocol
MIME: Multipurpose Internet mail extensions

8. **(c)**
DHCP is used to provide IP information to hosts on your network.

10. **(c)**
Domain name system converts given name to its IP address via a DNS server by using dnslookup, dig, or host.

11. **(d)**
1. It will send 4 message, and receive 4 response messages.
2. Since persistent HTTP leaves connection open if connection is not timeout and we don't close it. So we can send more webpages over persistent HTTP connection.

7 CHAPTER

Network Security

1. Consider a secured environment making use of symmetric key Cryptography. Every host connects every other host. Calculate the number of unique keys required (Symmetric Keys) if there are 5 hosts in the network.

2. Which of the following is the key sizes of DES and 3-DES respectively?
   1. 64, 128 2. 56, 112 3. 56, 168
   (a) Only 1 (b) Only 2
   (c) Only 3 (d) Both 2 and 3

3. Symmetric encryption algorithm is same as
   (a) RSA algorithm
   (b) Secure Hash Algorithm
   (c) Secret key encryption algorithm
   (d) Public key encryption algorithm

4. Which of the following is true regarding message digest?
   (a) It converts small data into large fixed-length string
   (b) Given P, No one can find P' such that MD(P') = MD(P) where P and P' are small numbers.
   (c) It is used to provide Confidentiality.
   (d) None of the above

5. Which of the following attack endangers the security of Diffie Hellman method if two parties are not authenticated to each other.
   (a) Man in the middle
   (b) Cipher text attack
   (b) Plaintext attack
   (d) None of these

6. Consider private key cryptosystem has 2 keys, 3 plaintexts and 4 ciphertexts.
   $k = \{k_1, k_2\}$
   $M = \{m_1, m_2, m_3\}$
   $C = \{C_1, C_2, C_3, C_4\}$
   Which of the following encryption table for (K, M, C) is valid?

   (a)

	m_1	m_2	m_3
k_1	c_1	c_3	c_4
k_2	c_2	c_4	c_2

   (b)

	m_1	m_2	m_3
k_1	c_1	c_2	c_4
k_2	c_2	c_4	c_1

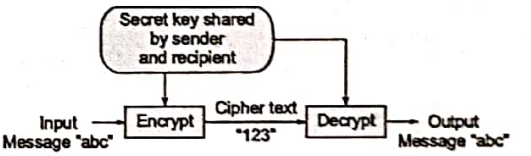
   (c)

	m_1	m_2
k_1	c_1	c_3
k_2	c_2	c_4

   (d)

	m_1	m_2
k_1	c_1	c_1
k_2	c_2	c_2

7. Consider the following cryptosystem



   Above cryptosystem is _____.
   (a) Symmetric key cryptosystem
   (b) Public key cryptosystem
   (c) Digital signature
   (d) None of these

8. Caesar Cipher is an example of
   (a) Data Encryption Standard (DES) algorithm
   (b) Monoalphabetic substitution
   (c) Polyalphabetic substitution
   (d) Block Cipher

9. Which of the following security services is/are not provided by digital signature?
   1. Authentication of message
   2. Integrity

3. Privacy
4. Non repudiation

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

10. Ram and Sita uses the Diffie-Hellman protocol for generating session key. Ram chooses $y = 3$ and Sita chooses $x = 5$. Identify session key value if $G = 7$ and $N = 23$

11. Two gate aspirants talking to each other use the RSA algorithm to encrypt their messages. They encrypt the message character by character. The value of p, q and d are 5, 17 and 13 respectively, where p, q and d are their integers having usual meaning in the RSA algorithm. Identify the sum of integers in cipher text for corresponding characters in plain text: "IIT". Assume that corresponding cipher characters are placed in their corresponding plain text character places. Also each character is converted to ASCII value before applying RSA (ASCII value of A, B, C,... and so on are 1, 2, 3,..., respectively).

12. The private key in public key encryption is used for

(a) encryption (b) hashing
(c) decryption (d) both (a) and (b)

13. Bob choosing 7 and 11 as P and Q respectively and choosen 'e' a random integer to be 13 the wants to send the plain text (M) is 5. The value of cipher text using RSA public cryptosystem is _____

■■■■

Answers Network Security

2. (d) 3. (c) 4. (d) 5. (a) 6. (b) 7. (a) 8. (b) 9. (a) 12. (c)

Explanations Network Security

1. **(10)**
If there are 'n' users the number of keys required is $\frac{n(n-1)}{2}$.

$\therefore \frac{5\times4}{2} = 10$ symmetric keys are required.

2. **(d)**
DES is a block cipher (operates on a fixed block of bits). It encrypts a 64-bit of plain text using a 64-bit key. But only 56 bits used as last bit of every byte is a parity bit.
DES uses 112 or 168 bits.

3. **(c)**
The secret key encryption alogrithm are often referred to as symmetric encryption alogrithms as the same key can be used in bidirectional communication between sender and receiver.

4. **(d)**
Converts large data into fixed size small data. P and P' should be large numbers it is used for authentication of data.

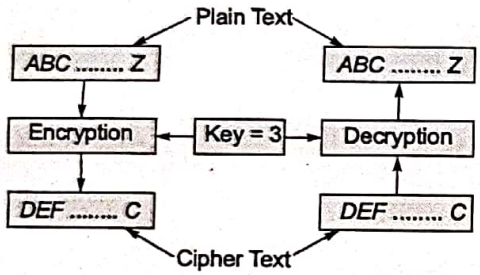
5. **(a)**
Sender thinks that he is communicating with receiver. Receiver thinks that he is communicating with sender with this attack, hacker communicates or mediates with sender and receiver.

6. **(b)**
Encryption function should be one to one
- $f_{k_2}(m_1) = f_{k_2}(m_3)$; not one to one
- All messages are mapped to unique cipher text using k_1 and k_2.
- for m_3 there is no mapping for k_1 and k_2
- for m_3 there is no mapping for k_1 and k_3

$\therefore$ Option (b) is correct.

7. **(a)**
Both sender and receiver can share the same key in symmetric key cryptosystem.

8. **(b)**
Monoalphabetic substitution is a symmetric key algorithm in which the relationship between characters in plain text is always one-to-one in Cipher text.
Caesar Cipher is an example of monoalphabetic substitution. In Caesar Cipher character in Cipher text is substituted by another character shifted by three places.
An example *A* is substituted by *D*.



9. **(a)**
Privacy is achieved using symmetric key cryptography (Public key-cryptography can also be used) Digital signature provide services of integrity, Authentication and non-repudiation. Using digital signature it is not possible to provid privacy.

10. **(14)**
Given $N = 23, G = 7$
$R_1 = G^x \bmod N$
$R_2 = G^y \bmod N$
$= 7^3 \bmod 23 = 21$
$= 7^5 \bmod 23 = 17$
$\therefore \quad K = (R_1)^y \bmod N$
$K = (R_2)^x \bmod N$
$= (21)^5 \bmod 23$
$= (17)^3 \bmod 23$
$= 4084101 \bmod 23$
$= 4913 \bmod 23 = 14$
$\therefore \quad K = 14$
Note: We can directly compute $G^{xy} \bmod n = 14$.

11. **(119)**
Given $p = 5, q = 17, d = 13$
$n = 85$
$z = (5-1)(17-1) = 64$
Here $d = 13$ is relatively prime to z
Now, $(e \times d) \bmod 64 = 1$
$\Rightarrow \quad e = 5$

P	$P^e \bmod n$	Cipher Character
I	$9^5 \bmod 85$	59
I	$9^5 \bmod 85$	59
T	$20^5 \bmod 85$	1

$\therefore$ Sum of integers in cipher text message:
$59 + 59 + 1 = 119$

12. **(c)**
The encryption algorithm and public key are publicly announced. The decryption algorithm and private key are kept secret.

13. **(26)**
$P = 7, Q = 11, e = 13$ and $M = 5$
$N = PQ = 7 \times 11 = 77$
$\phi = (P-1)(Q-1) = 6 \times 10 = 60$
$C = M^e \pmod N$
$= 5^{13} \bmod 77 = 26$

■■■■