TOPIC NAME : DAY : TIME : DATE : / /

1. (a)

(I) Given

1st usable IP : 109.64.0.1

Second last usable IP : 109.127.255.253

Last usable = +1 , So broadcast address will be +2

Broadcast address = 109.127.255.255

Network address = 109.64.0.0

$109.\underbrace{01}\underline{000000}.0.0.$ host bit

∴ ~~Subnet Mask~~ Network bit = 8+2 = 10

11111111.11000000.00000000.00000000

Subnet Mask in decimal = ~~255.192.0.0~~ 255.192.0.0

∴ Network address → 109.64.0.0/10

(II) Host bit = (32-10) = 22

∴ Total IP address = 2^{22} = 4194304

∴ Usable IP addresses = 4194304-2
= 4194302

TOPIC NAME :

32 16 8 4 2 1
1 0 0

DAY :

TIME : DATE : / /

1 (b) 109.64.0.0/10

Address	Closest possible host number	host bit	SN
2000+2	2048	11	3rd, 8
1400+2	2048	11	3rd, 8
4+2	8	3	~~1st~~ 4th, 8
2+2	4	2	~~1st~~ 4th, 4

1st. 109.64.0.0/21

2nd 109.64.8.0/21

3rd ~~109.64.8.8/29~~ 109.64.16.0/29

4th ~~109.64.8.12/30~~ 109.64.16.8/30

TOPIC NAME : DAY : TIME : DATE : / /

2 (a) TTL stands for time to live.

Every time a packet is passed through a router (hop) the router decreases the TTL value by 1. This is to end the endless routing of any packet.

128 is default ttl for windows.

$(128-104) = 24$

The packet hopped through 24 routers.

2 (b)

(i) fragments (MF=1)

Data per packet = 2883 - 35 = 2848 bytes

Total data for 10 packets = 2848×10 = 28480 bytes

Last fragment (MF=0)

Data = 985 - 35 = 950 bytes

Total original data size = (28480 + 950) = 29430 bytes

(ii) Packet 1: 2848 bytes offset 0

Packet 2: starts after the bytes of packet 1

$\therefore$ Offset $= \dfrac{2848}{8} = 356$

TOPIC NAME : DAY TIME : DATE : / /

2(b)
(ii) MF = 0 [No fragments will follow]

2 (e) Router R2 is not set up as a DHCP relay agent.

PC1 is connected with router R2. When the PC sends a broadcast message router R2 doesn't forward it to R3 (which is working as a DHCP server).

ip helper-address command on R2 would accept the broadcast message, forward it to R3. ~~and ma~~

3 (a) (i) Link state routing Algorithm. (Converges very fast with true shortest path)

(ii) We apply Dijkstra's algorithm starting from node 5

Set Node 5 cost to 0.

Current Node 5

to Node 4 0+1=1 Smallest cost in list : Node 4 (Cost 1)
to Node 6 0+2=2 1st Node visited = 4
to Node 8 0+6=6

Step 2: Analyzing Neighbours Node 4 (Current Cost 1)

To Node 0 1+3=4 Smallest Node 6 (cost 2)
2nd node visited Node 6
To Node 1 1+11=12
To Node 8 1+7=8 (~~So~~ we keep 6 as its the lowest)

TOPIC NAME : DAY : TIME : DATE : / /

Step 3: Analyze Neighbors of Node 6 (Current Cost 2)

To Node 2 : 2+4=6

To node 7 : 2+10=12

Smallest unvisited node : Node 0 (cost 4)

3rd Node Visited : Node 0

Step 4: Analyze neighbours of Node 0 (current cost 4)

to Node 1 : 4+4=8 (better)

Smallest unvisited node: Node 8 (cost 6)

Step 5: Analyze neighbours of Node 8 (current cost 6)

To Node 2: 6+2=8

Order	Node	Cost	Shortest Path
1	4	1	5 → 4
2	6	2	5 → 6
3	0	4	5 → 4 → 0
4	8	6	5 → 8
5	2	6	5 → 6 → 2

TOPIC NAME : DAY : TIME : DATE : / /

Q3 b) A Link-state algorithm uses the Hello Protocol to manage this process.

1. Discovery : Sends Hello Packet to Neighbour
2. Adjacency : ~~B~~ Two way relationship is added if neighbour responds
3. Sending : Once adjacency is established, the router will flood LSP to neighbour to synchronized LSDB

Q3 c)

In distance vector algorithm, explicit Hello packets are considered redundant because—

1. Periodic Updates : ~~These als~~ Entire routing table to neighbors at regular intervals.

2. Implicit keepalive : The routing update packet itself acts as a ~~ke~~ heartbeat.

Q4 (a) ip route 100.9.128.128 255.255.255.224 112.191.63.3

Q4 (b)

ip route 100.9.128.128 255.255.255.224 S1/1 5

Backup Route:

ip route 100.9.128.128 255.255.255.224 S1/0 10

TOPIC NAME : DAY : TIME : DATE : / /

Q4 (c) That is a next-hop IP address. this forces the router to perform a recursive lookup. This is less cpu efficient on point-point links.

Directly specifying the exit interface is more efficient.

ip route 21.1.64.0 255.255.255.192 s0/0

Q5 (a) In IPV6, intermediate routers do not fragment packets. If a router receives a package that is larger than the MTU:

1. The router drops the packet
2. The router sends a 'Packet too Big' error message back to source
3. The source the fragments the data and then retransmits.

Q5 (b) ~~Every~~ IPv6 uses Multicast. To send packets to all device on a local link, the packet is sent to All-Nodes multicast Address which is FF02::1

Q5 (c) Stateful DHCPV6.

DHCP server maintains a centralised database of all assigned IP address.

TOPIC NAME : DAY TIME : DATE : / /

6.(a)

1. OUI: The first 24 bits (3 bytes), assigned to the manufacturer.

2. NIC: The last 24 bits (3 bytes), unique to the specific device.

Bit Identification: The LSB of the first byte (octet) signifies the address type.

0 → Unicast   1 → Multicast

6. (b) No, because ARP operates only within local broadcast domain.

Host B, Host C and Router R1 will receive the ARP request

HostB and Router R1: Discard after checking

Host C: Update its ARP table and send a unicast ARP reply

6. (c) Switch SW1 (Unicasting):

→ SW1 receives the frame from Host A on port Fa0/1

→ Since the problem state SW1 already has the destination Mac address (Host D) in its table mapped ~~port~~ to port fa 0/3, SW1 performs a directed unicast.

TOPIC NAME : DAY : TIME : DATE : / /

Switch SW2 (Flooding):

→ SW2 receives the frame on port fa 0/1.

→ First SW2 learns the source MAC address (Host D). Since the table is empty, this is an unknown unicast. SW2 floods the frame out of all other active ports.

Updated MAC Address table

Switch SW1

00.90.21.D0.DD.48	Fa 0/1
00.0C.85.75.64.90	Fa 0/3

Switch SW2

00.90.21.D0.DD.48	Fa 0/1