1. (a)

(i) address range is 109.64.0.0 – 109.127.255.255

The block size in the 2nd octet is 64, which corresponds to /10.

subnet mask: 255.192.0.0 (/10)

Network address: 109.64.0.0

(ii) Host size,

Host bits = 32 – 10 = 32

Hosts = $2^{22} - 2 = 4,194,302$

(b) LAN – 2000 Hosts

Needs ≥ 2000 → /21

subnet size = $2^{11} - 2 = 2046$

11 Host bits

prefix = 32 – 11 = 21

mask = 255.255.248.0

Network : 109.64.0.0

② for LAN - 1400 Hosts, → /21

$2^{11} - 2 = 2046$ hosts

prefix = 32 - 11 = 21

Mask = 255.255.248.0

Network : 109.64.8.0

Switch network

needs ~ 4-5 IPs → /29 (6 usable

Network : 109.64.16.0

WAN link

Needs 2 hosts → /30

Network : 109.64.16.8

2.

(a) TTL is an 8-bit field in the IP header that limits how many routers a packet can pass through. Each router decrements TTL by 1. When TTL reaches 0, the packet is discarded.

So, TTL = 104 means the packet reached computer with 104 hops remaining.

(b) (i) Data per MF = 1 packet

$2883 - 35 = 2848$ bytes

Data in 10 such packets = $10 \times 2848 = 28480$

Data in last packet (MF = 0)

$985 - 35 = 950$ bytes.

Total origin = 28480 + 950 = **29430 bytes**

(ii) Data per fragment = 2848 bytes

offset is measured in 8 byte units

offset of 2nd packet = $\frac{2848}{8} = 356$

(iii) if MF flag = 0, this indicates no more fragments follow, so it is the final fragment of the original datagram.

(c) Reason: PC1's DHCP Discover is a Broadcast packet, and routers do not forward broadcasts by default. Since, PC1 is in subnet 192.168.4.0 and DHCP server is in a different subnet, the DHCP Discover stops at Router R2 and never reaches R3.

Solution: Configure DHCP relay on the router interface connected to PC1's network using an IP helper address pointing to R3's IP.

[3]

(a) i) The algorithm used in this topology is the Link-State Shortest Path Algorithm (Dijkstras Algorithm).

(ii)

order	Destina	shortest part	cost
1	4	5→4	1
2	6	5→6	2
3	0	5→6→0	4
4	8	5→8	6
5	2	5→6→2	6

(b) A router sends a Link state Packet to a neighbor only when it detects a change in its Local Link state, such as:

→ Link cost change

→ Link failure or recovery

→ New neighbor discoverd.

If, no change happens, no LLP is sent, which reduce unnessary traffic.

(c) Distance vector protocols do not use helb packet because neighbor existence and failure are detected implicitly through regular distance vector updates.

If updates stop arriving, the neighbor is

assumed to be unreachable.

[6]

(a) A MAC address has two parts:

① OUI (First 24 bits) → Identifies the manufacturer.

② NIC (Last 24 bits) → Uniquely identifies the device.

The LSB of first bytes indicates address type:

→ 0 = Unicast

→ 1 = Multicast

(b)

No, Host D is in a different network, and does not across routers, Host A will only learn the MAC address of its default gateway (R1).

The ARP request is broadcast and received by host B, C, R_1 and sw1.

→ Host C replies with its MAC address.

→ Host B and R1 ignore it.

→ sw1 floods the request within the LAN

(c) SW1 MAC table:

MAC addr	port
A	fa0/1
B	Fa 0/2
D	Fa0/3

SW2:

MAC add	port
A	fa0/1
D	Fa 0/3

When host A sends a packet to host D

→ SW1 knows D's MAC and forword the frame using unicast to SW2

→ SW2 does not know D's MAC, so it floods the frame.

→ SW2 learns A's MAC from the incoming frame and later learns D's MAC from the reply.

[4] (a) LAN C = 100.9.128.128/27

Router C's IP on the Multi-acces network is

→ 112.191.63.3

static router on R-B:

IP route 100.9.128.128 255.255.255.224

112.191.63.3

(b)

Primary static route on Route A with AD = 5 using S1/1:

ip route 100.9.128.128. 255.255.255.224 S1/1 5

If the links fails, using a floating static route with higher AD:

ip route 100.9.128. 255.255.255.224 112. 23. 224.161.10

(c) The route S 21.1.64.0/26 via 112.23 .224.162 is not recommended because it causes recursive routing. It should be changed to use an exit interface or directly connected next hop.

ip route 21.1.64.0 255.255.255.192 50/1

5

(a) IPv6 do routers do not perform fragmentation. If a packet exceeds the MTU, the router drops the packet and sends an ICMPv6 "Packet too Big" message to the source. The source host performs fragmentation using the fragment Extension header. Router add extra information using IPv6 Extension headers instead of modifying the base header.

(b) IPv6 does not support broadcast.

Broadcast functionality is achieved using multicast address.

(c) stateful DHCPv6 does not require DAD. Because the DHCPv6 server assigns unique IPv6 address, duplication in not possible.