Q1 i. Network bits = 17 ; Host bits = 32 - 17
= 15 bits

∴ Total Host = $2^{15} \times 2$
= 32766

ii. Subnet mask = 255.255.128.0

3rd octet block size = 128 [0-127]

Network address = 32.99.0.0

∴ Broadcast address = 32.99.127.255

iii.

Network	Required host	Host bits	Subnet	Network address
LAN A	2000	11	121	32.99.0.0
LAN B	1024	10	122	32.99.8.0
LAN C	3	2	123	32.99.12.0
WAN 1	2	2	130	32.99.12.8
WAN 2	2	2	131	32.99.12.12

Q2 I To allow external users to initiate FTP access (port 21) to an internal server static NAT with port forwarding is required.

Public IP 203.0.113.10:21

Internal 10.0.0.50:21

II It is using PAT because: . One public IP
. Multiple internal users borrowing simultaneously
. port number used to differentiate sessions

3. I. $n = \frac{6397}{1624} = 3.94 \approx 4$

II. $6397 - (1624 \times 3) = 1525$

III. fragment offset of last fragment $= \frac{16293}{8} = \frac{4872}{8} = 609$

[offset value in 8 byte units]

IV. Reassembly of destination –

Uses: Source IP, Destination IP, Identification field.

- fragments reordered using fragment offset.
- MF flag tells when last fragment arrives
- Packet is reassembled only when all fragments arrive.

V. Significance of MF flag:-

MF = 1 → more fragment coming

MF = 0 → last fragment.

Q5 R_1, R_4 and ISP router will converge faster because they run a Link state Protocol.
- Routers build a complete topology map.
- Changes are flooded immediately.
- No Periodic full-table updates.

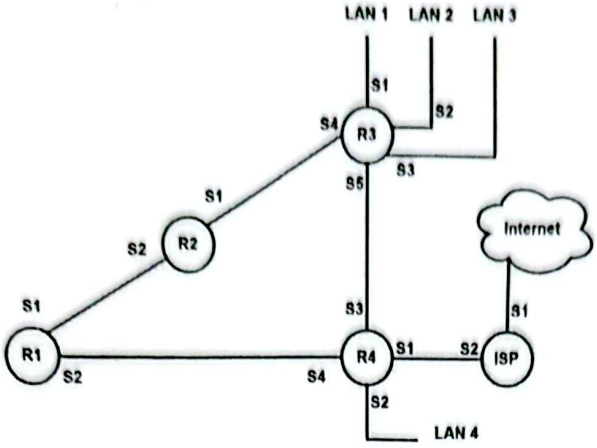
Distance Vector	Link state
• Track Neighbors implicitly	• Track neighbours explicitly
- Learn via:	• Use: Hello Packets
Routing table updates	Neighbor table
Incoming Interface	Link state Database (LSDB)
No explicit neighbour table	

Q7 I Source MAC = PC A's MAC Destination MAC = FF:FF:FF:FF:FF:FF (Broadcast)

II

[CO3] SECTION B [Answer ANY TWO out of THREE in this section] - 12 MARKS

Q4



Device	Interface	IP	Network
R1	S1	.101	192.168.10.100/30
	S2	.225	192.168.11.224/30
R2	S1	.193	192.168.12.192/30
	S2	.102	192.168.10.100/30
R3	S1	.1	192.168.96.0/24
	S2	.1	192.168.64.0/25
	S3	.1	192.168.80.0/26
	S4	.194	192.168.12.192/30
	S5	.97	192.168.10.96/30
R4	S1	.1	192.168.9.0/30
	S2	.1	192.168.72.0/27
	S3	.98	192.168.10.96/30
	S4	.226	192.168.11.224/30
ISP	S1	.1	210.1.1.0/24
	S2	.2	192.168.9.0/30

Given the following topology where R1-R4 denote routers and the respective IP table of the topology. 3 + 3

I. **Configure** a **directly attached default** static route in **R2** with **AD = 10**.

II. **Configure** a **backup** route of the above default static route using the next hop IP address.

Q5 Referring to the **Q4's** topology, **R1, R2 and R3** are running Distance Vector protocol and **R1,R4 and the ISP router** are running Link State Protocol. **Determine** which routers will converge faster and **why**. Also, **state** which routers will keep track of their neighbors and **how**. 3 + 3

Q6 **Write** the shortened version of the following IPv6 addresses: 6

I. 2001:0db8:85a3:0000:0000:8a2e:0370:7334 2001:db8:85a3::8a2e:370:7334

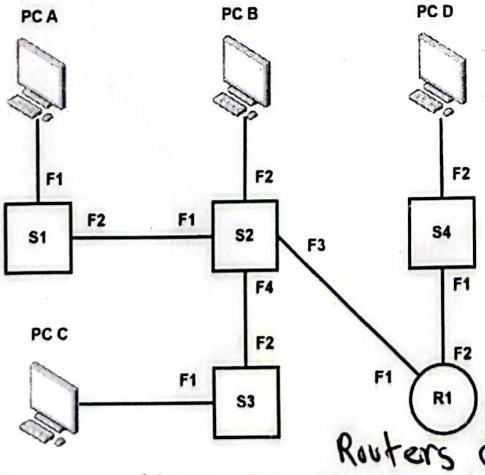
II. 2607:0000:0000:0805:0000:0000:0000:200e 2607:0:0:805::200e

III. 3ffe:1900:4545:1003:1200:a0f8:fe21:67cf 3ffe:1900:4545:1003:1200:a0f8:fe21:67cf (no compression possible)

END OF SECTION B

[CO2] SECTION C [Answer ANY THREE out of FIVE in this section] - 18 MARKS

Q7



Refer to the figure, **PC A** sends an ARP requests for **PC D**. 2 + 2 + 2

I. **State** the **source** and **destination** MAC addresses in the ARP request packet.

II. **State** what will router **R1** do with the packet and **why**.

III. After receiving the ARP reply, **state** what is the first action made by **PC A**.

II Router R1 will drop the ARP Packet.
Because: ARP is a Layer 2 Broadcast.
Routers do not forward broadcast packets.

III PC A:
- Stores MAC-IP mapping in ARP cache.
- Sends the data frame to PC D.

I MAC-Source = PC A's MAC address

MAC-Destination = FF:FF:FF:FF:FF:FF (Broadcast)

Q8 Consider a situation where someone is involved in malicious activities in our USIS system. The system administrator detected the source socket address associated with these actions. Despite this, they could not pinpoint the specific user due to the absence of end-to-end traceability. **Discuss** and **evaluate** the potential factors that could have contributed to the loss of this traceability. 6

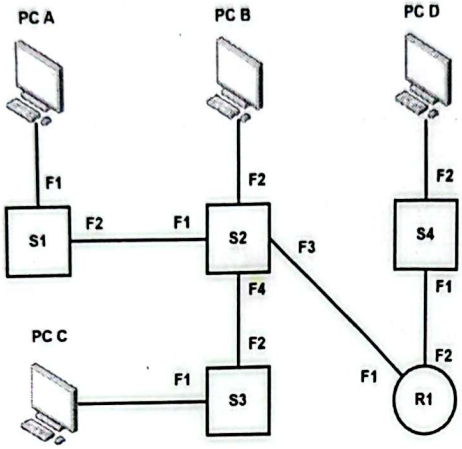
Q9 In a DHCP-enabled network, each IP address is assigned to a device for a specific period, known as the lease time. Upon expiration of this lease, the device must renew its IP address to maintain network connectivity. 2 + 4

I. **List** the steps involved in the IP address **renewal** process with DHCP.

II. Additionally, **discuss** potential reasons a device might fail to renew its IP address. **Mention** which actions the device takes if it cannot renew the IP address.

Q10 **Explain** the function of the **loopback address** in network communications. Additionally, **provide** the loopback address used in IPv4 and IPv6. 4 + 2

Q11



Refer to the figure given, **PC A** sends a packet to **PC C**, at this stage all switch tables contain information about all devices shown. No worries!! 4 + 2

I. **State** the actions that the switch **S2** will take after it receives the packet.

II. **Explain**, using the above scenario, why we call switches to be self learning.

END OF SECTION C

THE END

Why did the computer network go to therapy?
It had too many unresolved IP issues.

Q11 I Switch S2 Packet Handling:
- Reads Source MAC
- updates MAC table
- Looks up destination MAC
- Forwards packet via correct port (No flooding since table is complete)

II
- Learn MAC's from incoming frames
- No manual configuration needed
- Automatically updates table

Q10 It is used to send and verify ~~the~~ and test the proper functioning of the networking stack on a local device without sending packets to the external network. It allows a computer to send network packets to itself, which helps in trouble shooting diagonistics, and testing network applications. Packet sends to the loopback address never leave the host and are immediately routed

back internally. IPv4: 127.0.0.1 IPv6: ::1