(1) i) Here,

Network bits = 17

Host bits = 32 - 17 = 15

∴ Total hosts = $2^{15} - 2 = 32766$

ii) Subnet mask = 255.255.128.0

Third octate block size = 128 (range 0 - 127)

Network address = 32.99.0.0

∴ Broadcast address: 32.99.127.255

iii)

Network	Required Hosts	Host bits	Subnet	Network address
LAN A	2000	11	/21	32.99.0.0
LAN B	1024	10	/22	32.99.8.0
LAN C	23	2	/29	32.99.12.0
WAN 1	2	2	/30	32.99.12.8
WAN 2	2	2	/30	32.99.12.12

(2) 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 browsing simultaneously
- Port numbers used to differentiate sessions

(3) i) Number of fragments = $\frac{6397}{1624} = 3.94$

≈ 4 fragments

ii) Data size of last fragment = 6397 (16243)

= 1525 bytes

iii) Fragment offset of last fragment:

$$\frac{11243}{8} = \frac{4872}{8} = 609$$

[offsets are in 8 byte units]

iv) Reassembly at 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 fragments coming

MF = 0 → Last fragment

(4) i) ip route 0.0.0.0.0.0.0.0 <exit-interface> 10

ii) ip route 0.0.0.0.0.0.0.0 <next hop-IP> 20

(5) Link state routers (R1, R4, ISP). Because-

- Full topology knowledge
- SPF algorithm
- Event-triggered updates

Distance vector: via periodic routing updates

Link State: via Hello packets & LSPB

(6) i) 2001:db8:85a3::8a2e:370:7334

ii) 2107::805:0:0:200e → 2107:0:805:0:200e

iii) 3ffe:1900:4545:1003:1200:a0f8:fe21:67cf

(7) i) Source MAC → PC A

Destination MAC → FF:FF:FF:FF:FF:FF

ii) Router 1 - Drops packet

- Routers do not forward broadcasts

iii) First action after ARP reply:

- PC A updates ARP table
- Sends actual data packet

(8) Possible causes:

- NAT/PAT masking users
- Dynamic IP addressing
- Proxy servers
- VPN tunneling
- Lack of logging
- Shared credentials

(9) i) Steps - DHCPREQUEST
- DHCPACK

ii) Renewal failure reasons -

- DHCP server down
- Network issue
- Lease expired
- Address conflict

If renewal fails:

- Device uses APIPA (169.254.x.x)

(10) Function - Tests TCP/IP stack

- Local communication

- Troubleshooting

Address - IPV4; 127.0.0.1

IPV6; ::1

(11) i) S2 Actions:

- Checks MAC table

- Forwards to connect port

- Does not flood

ii) Switches are self-learning;

- Learns MAC → Port mapping from incoming frames

- Automatically build forwarding table.