1024+1024+512 = 2560 Address

1)i) Original /19 = 8192 Address [lots of space left].

$32-19=13$

$\frac{2^{13}}{2^{2}} = 2^{13-2} = 2^{11}$

(Ans)

ii) NA = 3.255.192.0/22

from smallest to largest → R1 (hosts 1000) = 1000 + 2 = 1002

R2 (hosts 512) = 512 + 2 = 514

R3 (hosts 255) = 255+2 = 257

R1 →	1002	$\log_2 1002 = 10$	32 - 10 = 22	3rd (4)	3.255.192.0/22
R2 →	514	$\log_2 514 = 10$	32 - 10 = 22	3rd (4)	3.255.196.0/22
R3 →	257	$\log_2 257 = 9$	32 - 9 = 23	3rd (2)	3.255.200.0/23

Hierarchical tree diagram:

3.255.192.0/19

(Range: 192.0 - 223.255)

Subnet R1

3.255.192.0/22

(192.0 – 195.255)

Subnet R2

3.255.196.0/22

(196.0 - 199.255)

Subnet R3

3.255.200.0/23

(200.0 - 201.255)

2) i) LAN 5 : 198.44.128.0/20 (Binary 3rd Octet : 10000000)

LAN 6 : 198.44.144.0/20 (Binary 3rd Octet : 10010000)

LAN 7 : 198.44.160.0/20 (Binary 3rd Octet : 10100000)

LAN 8 : 198.44.176.0/20 (Binary 3rd Octet : 10110000)

the networks span from 198.44.128.0 to 198.44.191.255.

This is a block of 64 (2^6) in the third octet.

Mask = (/24 − 6 = /18) or (/20 − 2 = /18)

∴ Summarized Address : 198.44.128.0/18

command on R1 : ip route 198.44.128.0 255.255.192.0 20.2.1.2

ii) Current Primary : via S1 interface (connecting to R2).

Backup path : S0 interface (connecting directly to R1).

Floating route : must have higher AD than the primary

next hop : R1's interface S1[.1] IP is 20.2.2.1

command : ip route 0.0.0.0 0.0.0.0 20.2.2.1 50

3) i) MTU = 540 bytes

data payload = 4080 bytes

IP header = 20 bytes

$\therefore$ max payload per fragment = $(540 - 20)$ = 520 bytes

$\therefore$ No of fragments = $\frac{4080}{520} \approx 7.84$

$\therefore$ 8 fragments.

(Ans)

ii) Total data bytes preceding the 4th fragment:

(3×520) bytes / fragments

= 1560 "

offset = $\frac{1560}{8} = 195$

(Ans)

iii) Since the 4th fragment is not the last fragment as there are total 8 fragments, so the MF bit is set to 1.

(Ans)

4) Source MAC : the mac address of the wifi router.

Destination MAC : the mac address of my mobile or

Broadcast (FF:FF:FF:FF:FF:FF)

Content : IP address offered, Subnet Mask, Gateway IP,

DNS Server, Lease time.

Reply: My mobile will broadcast a DHCP Request message

formally requesting to lease the offered IP address.

5) Dipu can communicate with the private web server because

R2 is configured with Port forwarding (Static NAT).

R2 maps a specific port like 8080 on it's public IP

(201.113.13.221) to the private IP (192.168.1.2) and port 80

of the web server. Dipu sends packets to 201.113.13.221:8080.

R2 intercept this, translates the destination IP/Port to

192.168.1.2:80 and forwards it to the server.

6) Routers R3 knows to send LSP packets only to interfaces S1 and S0 because LSPs are only exchanged between routers to build the topology map. The others interfaces from "F0 to F3" are connected to LANs (end devices or passive interface where no other OSPF neighbors to form adjacencies with. So, flooding LSPs onto the LANs is unnecessary and inefficient.

7) IPV6 = 2000::B0B:80 :A8FF : FE03 :4566

using EUI-64 pattern A8FF:FE03. The FF, FE is inserted in the middle of MAC, so removing these, A8, 03

Last 64 bits ⇒ 0080 : A8FF : FE03 : 4566

first half → 00 80 A8

Second half → 03 45 66

Converting 7th bit of first Byte

0000 0000 → 00000010 → 02 (converting to Hexa Decimal)

So, MAC address → 02 : 80 : A8 : 03 : 45 : 66

11) 2000:0000:0000:0B0B:0080:A8FF:FE03:4566

the subnet ID is typically the 4th hextet.

Subnet ID: 0B0B

(Ans)

S1:

8) S1 checks its MAC table as it its empty, it adds an entry,

PC2 is on Port F1. ~~S1 checks for the~~

Forwarding: S1 checks for the destination MAC addresses PC4 and PC6. Since the table is empty, S1 floods the frames.

Result: S1 forwards the frames out of all ports except the incoming port. Sent out of F0 (towards PC1), sent out of F2 (towards S2).

S3:

PC2's Frame (Incoming): The frame from PC2 travels S1→S2→S3. S3 receives it on F0. So, S3 learns PC2 is on interface F0.

PC6's Reply (Incoming): PC6 replies. The frame travels S4→S3. S3 receives it on F3. S3 learns PC6 is on interface F3.

PC4: Since PC4 does not reply, S3 never receives a frame with PC4 as the source. So, it doesn't learn PC4's address.

MA	Interface
PC2	F0
PC6	F3

S4:

PC2's frame (Incoming): The frame travels S1→S2→S3→S4. S4 receives it on F0. S4 learns PC2 is on interface F0.

PC6's Reply (Incoming): PC6 directly connected to S4 and sends the reply. S4 receives it on F1. S4 learns PC6 is on interface F1.

MA	Interface
PC2	F0
PC6	F1

(9) The Administrative Distance (AD) indicates trustworthiness (lower is better). LSP has a lower AD(90) than RIP(120) because it is a more reliable and sophisticated protocol. LSP uses a full map of the network (topology) and metrics like bandwidth

to calculate the best path, ensuring loop-free and efficient routing. RIP relies solely on hop count (ignoring link speed) and is prone to routing loops making it less trustworthy.

10) Entries have Time-To-Live (TTL) so that the ARP cache is refreshed periodically. This ensures that if a device changes its network card or IP address the table updates to prevent connection errors.

Routers do not forward ARP requests because ARP is a Layer 2 Broadcast protocol. Routers create boundaries between broadcast domain, forwarding them would flood the entire inter. with local traffic.

11) IPv6 handles extra information using extension headers. Instead of variable length main headers, IPv6 keeps the main header fixed at 40 bytes. If extra info is needed the 'Next Header' field points to an extension Header (like hop by hop options) located between IP header and the payload. The payload length field in the main header

is updated to include the size of these extension headers.

12) i) MAC Address : AF : CC : FE : 12 : 23 : 40

First byte AF (Hex) = 1010 1111 (Binary)

the second least significant bit is the U/L bit. It is 1.

So, the address is locally administered.

ii) A MAC address is physically burned into the Network Interface card hardware by the manufacturer. It does not change based on the network connection or location (unlike IP address). So, if anyone move the device/NIC to a different network, the MAC address remains the same, making it portable with the hardware.

13) I can see the IP address (and hostname if resolved) of every router along the path to the destination and the Round Trip Time for packets to reach each hop.

Troubleshooting helps identify network congestion or connectivity breaks. Like if traceroute stops at hop 5, user know the connection breaks between hop 5 and 6. It also reveals latency bottlenecks if the time spikes significantly at a specific hop.