Assignment-2

Name: Md. Shakhawat Hossain

ID : 22201960

Section: 22

Faculty: BIJS

Spring 24 (A)

final

Answer : to the Q NO ⇒ (01)

i) Root network : 3.255.192.0/19

Here, 32 - 19 = 13 host bits

∴ Max subnet = [illegible] = [illegible]

Based on topology the max subnet = $2^{11} = 2048$

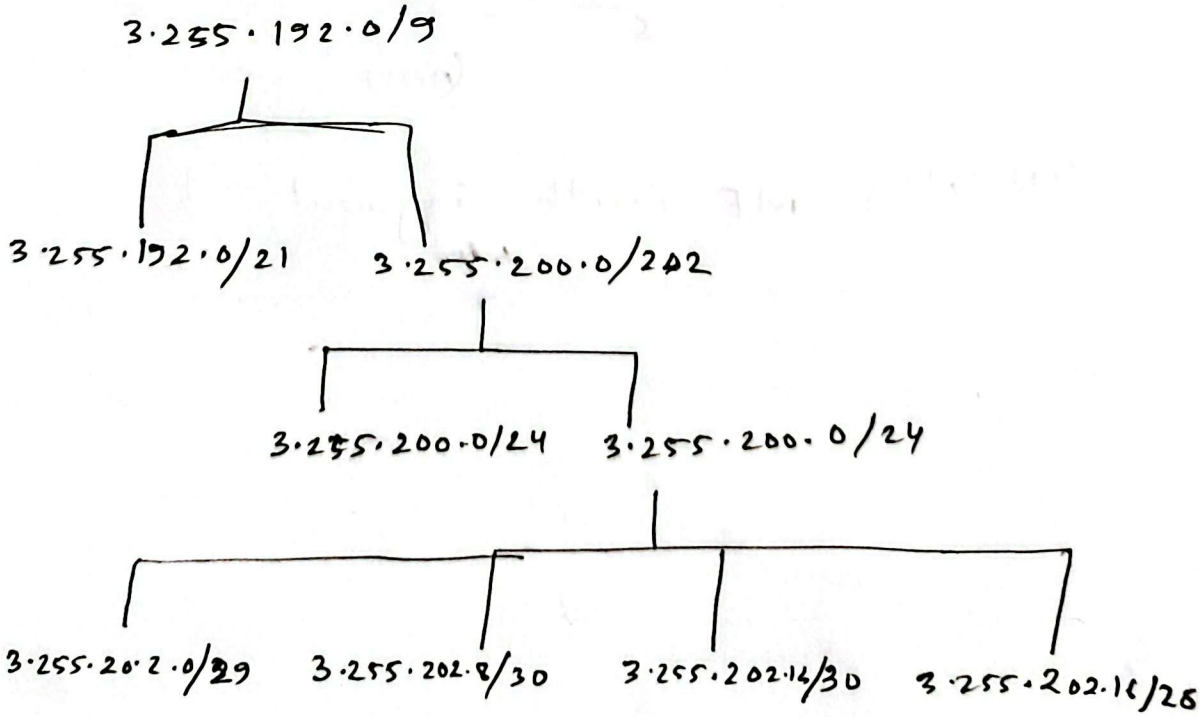
(ii) Root : 3.255.192.0/19 First level :

3.255.196.0
3.255.200.0

second ~~first~~ level subnets :

3.255.202.0
3.255.202.8
3.255.202.12
3.255.202.16

Tree :



Answer: to the Q NO ⇒(ii)

Network	3rd octet
198.44.128.0	10000000
198.44.144.0	10010000
198.44.160.0	10100000
198.44.176.0	10110000

2bit

Common bit, (16+2) = 18

Summarized network = 198.44.128.0/18

subnet mask = 255.255.192.0

Static route on R_1:

R_1(config) # ip route 198.44.128.0 255.255.192.0 20.2.1.2

(ii)

R3 config # ip route 0.0.0.0 0.0.0.0 20.2.2.1 5

Answer : to Q NO ⇒ (03)

(i) Soln:

Each full fragment = 520 bytes

Data size = 4080

$\therefore \frac{4080}{520}$ → remainder 7

Now, $4080 - 7 \times 520 = 440$

So, 7 full fragment + 1 last fragment = 8 fragment

(ii) Soln:

Data per full fragment = 520 bytes in

$= \frac{520}{8} = 65$ byte (in 8 bytes)

4th starts after 3 full fragment = $3 \times 520 = 1560$

$\therefore$ Offset = $\frac{1560}{6} = \underline{195}$

(Ans:)

(iii) Soln: MF fourth fragment = 1

Ans: to Q No ⇒ 64)

DHCP offer frame is sent by wi-fi router / DHCP server to client that still has no IP, so dest. is typically broadcast MAC FF:FF:FF:FF:FF:FF.

After receiving it the mobile replies with a DHCP request to accept that offer and then the server sends DHCPACK to confirm.

Answer to the Q NO ⇒ 65):

Dipu reaches the private web server by connecting to R2's public IP, not the server's private IP.

R2 uses destination NAT/port forward to translate inbound traffic on a public port to the web server's private IP and port inside the LAN.

When the server replies, R2 translates the addresses back so the response returns to Dipu correctly, even though the server itself has no public IP.

Answer : to the Q NO ⇒ (6)

R_3 sends LSPs only on s0 and s1 because link state protocols first discover neighbours on each interface using Hello messages, & LSP flooding happens only over interfaces where an adjacency / neighbour relationship exists.

So if R_3 has working adjacencies only on s0 & s1, it will flood LSPs only ~~out~~ the surface.

Answer : to the Q NO ⇒ (7)

Given IPv6 → 2000::BOB:80:A8FF:FE03:4566

(i) MAC address

Interface ID part = A8FF:FE03:4566

~~for EUI-64, remove~~

Final MAC address: AA:??:??:03:045:66.

(ii) Subnet IP:

Subnet is ~~64~~ first 64 bits = 2000::/64

Answer Q.10:

ARP cache entries age out so devices don't keep stale IP → MAC mappings when host move, reboot, change NICs. or when switch relearns paths.

ARP is a link-layer/ broadcast-domain protocol and routers seperate broadcast domains so ARP stays within the local subnet & it's not rounted across networks.

Answer Q(12):

Given MAC: AF:CC:FE:12:23:40

(i) First octet = AF = 1010 1111

U/L bit is 1 so it is locally administered address not globally unique.

(ii) A MAC address is Layer -2 identifier used for hop-to-hop delleverey on local link, it is not tied to an IP network/prefix like an IP address.

So, a device can move to a different IP network and change IP addresses while interfaces MAC typically stays the same, making it portable across networks.

Answer to Q 13:

Traceroute shows each hop on the path to Yahoo, usually with the hop's IP/hostname & round-trip times (RTT) for a few probes, timeout often appear as *.

It helps troubleshooting by pinpointing where latency jumps or where packets stop getting replies, so problematic link/router segment can be identified.