Name: Sadia Hakim Mollik

Student ID: 22201674

Section: 23

Assignment No: 02 (Spring 2025-A)

Answer of 01:

① Broadcast address: 7.16.255.255/18

Subnet mask = /18

Host bits = 14

ranges:

7.16.0.0 – 7.16.63.255

7.16.64.0 – 7.16.127.255

7.16.128.0 – 7.16.191.255

7.16.192.0 – 7.16.255.255

network address = 7.16.192.0/18

(ii)

LAN	Hosts
R2	2500
SW	125
R4	64

For R2 ⇒

$2^{12} - 2 = 4094$

Subnet:

Network: 7.16.192.0/20

Range: 7.16.192.1 – 7.16.207.254

Broadcast: 7.16.207.255

For SW ⇒

$2^7 - 2 = 126$

Next available network:

Network: 7.16.208.0/25

Range: 7.16.208.1 – 7.16.208.126

Broadcast: 7.16.208.127

For R4 ⇒

$2^7 - 2 = 126$

Next available network:

Network: 7.16.208.128/25

Range: 7.16.208.129 – 7.16.208.254

Broadcast: 7.16.208.255

(iii) Total usable IPs /25 = 126

Host = ~~64~~ 63

Wasted IP = 126 – ~~64~~ 63 = ~~62~~ 61 IP addreses.

Answer of 02:

① PC D LAN = 191.46.42.20/28

Network address: 191.46.42.16/28

R2 – R3 = 191.54.20.128/25

The networks:

191.46.42.16/28

191.54.20.128/25

194.52.10.11

(ii) ip route 192.52.64.12 255.255.255.252 S0/0/0 50

(iii) ip route 0.0.0.0 0.0.0.0 192.64.52.2

(iv) Default Static route AD = 1

Backup route must have higher AD. The backup next hop ∅ is the IP address of R2 on the R1-R2 link. This provides an alternate path to the ISP via R2 and R3 when the primary ISP link fails.

(v) R4 discards the packet because it has no matching route for the destination network 172.42.10.4 in its routing table. As a result, the routing lookup fails and the packet is dropped.

Answer of 03:

Total packet = 2584 bytes.
Header = 32 bytes
Payload = 2552 bytes
4th fragment size = 272 bytes
MF = 1

(i) MTU = 272 - 32 = 240 bytes

∴ MTU = 272 bytes.

(iii) Fragment offset for the 7th packet ⇒

$$\frac{6 \times 240}{8} = 180.$$

(iv) Total fragments ⇒

$$\frac{2552}{240} = 10.63 \approx 11$$

Answer of Q4:

R2 determines its neighbors by examining its directly connected interfaces, routers connected on those links are considered neighbors. In the first iteration of the Distance Vector Algorithm, R2 sends to its neighbors (R1 and R3) information about only its directly connected networks, each with a hop count of 1.

Interface	connected to
g0/1	PC A
g0/0	PC B
S0/1/0	R1
S0/0/0	R3

The neighbors of R2 are R1 and R3.

Directly connected network of R2.

Network	Source
192.152.10.0/16	PCA
192.141.10.0/24	PCB
R2-R1	WAN
R2-R3	WAN

in the first iteration, a router sends only its directly connected networks with distance 1 hop to all neighbors.

Answer of 05.

① 2001:0db8:12af:0000:0000:0000:0020:0004
Shortest form:
2001:db8:12af::20:4
type: Global unicast address.
purpose: used for unique, routable addresses on the IPv6 internet for end to end communication.

② 0000:0000:0000:0000:0000:0000:0000:0001
Shortest form: ::1
type: Loopback address
purpose: used by a device to send packets to itself for testing and troubleshooting.

Answer of 06:

① The computer cannot ping the internet server.
Because: ① Default gateway or routing problem.
② Firewall or ICMP blocking.

② A network administrator can use ICMP tools to identify wheather the issue is internal ~~within~~ inside or outside of the campus.

① Ping: Pinging the default gateway could be a way. If this fails, the problem is inside the campus network.
Pinging a known external IP address is another way. If internal pings works but external ping fail, the issue is likely outside the local network or at the campus internet gateway or firewall.

② Traceroute: It shows the path packets take from the lab computer to the destination. If the trace stop at a campus router, the problem is within the campus network. If it pases campus routers and fails later, the issue is outside the campus network.

Answer of 07:

① The Fragment offset field does not count bytes directly. Instead, it represents the offset in units of 8 bytes.
Each fragment's data except the last one is multiple of 8 bytes. The 13 bit value indicates how many 8 byte blocks precede the fragments. Because of this,
maximum offset $= 2^{13} - 1 = 8191$
maximum data size $= 8191 \times 8$
$= 65528$ bytes.
This matches the maximum IPV4 packet size defined by the 16 bit total Length field. So, The fragment's position is represented accurately without loosing information.

(11) The identification field is used to uniquely identify all fragments belonging to the same original IP packet. When a packet is fragmented, all fragments carry the same identification value. At the destination, the server uses ⇒

→ Source IP
→ Destination IP
→ Protocol
→ Identification field.

without this field, fragments from different packets could be mixed up during reassembly.

Answer of 08:

① When a PC first connects to a DHCP-enabled network, it does not have an IP address and it does not know the IP address of any DHCP servers.
So, it sends a DHCP discover message as a broadcast:
Source IP: 0.0.0.0
Destination IP: 255.255.255.255

② The PC receive DHCP offer.
The DHCP server responds with offered IP address, subnet mask, default gateway, DNS server, lease duration.
DHCP request is now the PC replies. It accept the offered IP address and inform all DHCP servers which offer it has chosen.
The selected server confirms the lease, and the PC configures its network setting.

Answer of 09:

① The recruiter can not access the server because –

– The web server is hosted on a private IP address which is not routable on the internet.

– The router uses NAT, which by default allow outbound ~~con~~ connections only from inside the lab.

– There is no mapping telling the router to forward incoming traffic from the public IP to the internal server on port 8080.

So, when the recruiter tries to connect to the public IP, the router does not know which internal device should receive the request and drops the traffic.

② The router must be configured with port Forwarding. Required set up ⇒

– Public IP : <router_public_IP>
– Public port : 8080
– Private IP : 10.10.5.50
– Private port : 8080
– Protocol : TCP

The configuration forwards incoming requests from the internet to the internal web server.

Answer of 10:

IPV6 has a larger base header than IPV4, it improves efficiency in several ways ⇒

(i) Simplified fixed-length header.
(ii) No fragmentation by routers.
(iii) Extension headers instead of optional fields.
(iv) Improved flow handling.
(v) Efficient routing and scalability.

Answer of 11:

(i) ARP Request Generation by Host A:
Host A wants to communicate with host C. Host A knows Host C's IP (192.168.1.20) but does not know its MAC. ARP request packet:
Source MAC: AA-AA-AA-AA-AA-AA
Destination MAC: FF-FF-FF-FF-FF-FF
Source IP: 192.168.1.10
Destination IP: 192.168.1.20
This is a broadcast frame sent to all devices in the local network.

Switch S1 processing:
S1 receives the ARP request on port F1. S1 records Host A's MAC on port F1 in its MAC Table.

As the destination MAC is broadcast, S1 floody the packet to all other ports except F1:

- Forward to F2 (Host B)
- Forward to F3 (link to S2)

Switch S2 processing:

S2 receives the ARP request on port F3, S2 records the MAC of the sender on port F8. As the packect is broadcast, S2 floody it to all the other ports except F3: Forward to F4 (Host C).

Host response:

Host B receives the ARP request but ignores it because the IP does not match. Host C receives the ARP request and replies with an ARP reply:

Source MAC: CC-CC-CC-CC-CC-CC

Destination MAC: AA-AA-AA-AA-AA-AA

Source IP: 192.168.1.20

destination IP: 192.168.1.10

Switches S2 and S1 learny Host C's MAC and update their tables. The reply is unicast back to Host A using the MAC tables.

(11) Switches are called plug-and-play because →

- They Automatically learns the MAC address of connected devices.
- No manual configuration of MAC address on ports is required.
- They forward Traffic intelligently using their MAC tables, reducing unnecessary network flooding after initial learning.
- This makes the networks easy to set up and manage.