Time : Date :

Assignment - 02

Name: Noity Karim

ID : 22201345

Course : CSE 421

section : 22

Assigned Question: Spring 2025 (Final)

Set : A

Day :

Time : Date : / /

Answer to the Question No - 01

1/(i)

Given,

broadcast address : 7.16.255.255/18

here subnet mask = 255.255.192.0

Block size in 3rd octet = 256-192 = 64

3rd octet of given broadcast = 255

Subnets in 3rd octet → 0, 64, 128, 192

∴ Network address = 7.16.192.0/18 (Ans)

1/(ii)

largest = R2 LAN 2500 hosts

R3 LAN 125 hosts

R4 LAN 64 hosts

Subnet	Hosts Needed	CIDR	Net Add	Usable Range
R2 LAN	2500	/20	7.16.192.0/20	7.16.192.1 - 7.16.207.254
R3 LAN	125	/25	7.16.208.0/25	7.16.208.1 - 7.16.208.126
R4 LAN	64	/25	7.16.208.128/25	7.16.208.129 - 7.16.208.254
WAN R1-R2	2	/30	7.16.209.0/30	7.16.209.1 - 7.16.209.2
WAN R1-R3	2	/30	7.16.209.4/30	7.16.209.5 - 7.16.209.6
WAN R1-R4	2	/30	7.16.209.8/30	7.16.209.9 - 7.16.209.10

Day :
Time : Date : / /

1/(iii)

R4 LAN : /25 subnet

-total addresses = 128

usable = 126

Hosts needed = 64

Wasted usable IPs = 126 - 64 = 62

(Ans)

Answer to the Question No - 02

2/(i)

R3's interface to R2 : 191.54.20.129/25

Network = 192.54.20.128/25

R3's interface to PC E : 194.52.10.11/15

Network = 194.52.0.0/15

Directly connected networks in R3's routing table:

191.54.20.128/25

194.52.0.0/15

(Ans)

2/(ii)

R2 connected to R1 via s0/0/0 but directly attached static route means we use exit interface not next-hop ip.

ip route 192.44.0.0 255.255.0.0 s0/0/0 50

Day :
Time : Date : / /

2/(iii)

here S means default route.

Recursive static route = next hop IP

∴ IP route 0.0.0.0 0.0.0.0 192.54.52.1 → default static route.

(Ans)

2/(iv)

A backup static route would have higher AD than default static. AD = 1

AD > 1 for backup

∴ AD = 200

(Ans)

2/(v)

172.42.10.4 is in the 172.16.0.0/12 private IP range and these IP's are not routable on the internet if R4 doesn't have a route to it it will discard it.

172.42.10.4 is a private IP address and R4 has no route to it so it discards the packet.

(Ans)

Day: _____

Time: Date: / /

Answer to the Question No -03

3/(i)

Given,

9th fragment size = 272 bytes (data = 240, header = 32)

For non-last fragments data size multiple of 8.

X = fragment size when full = 272 byts.

MTU X = 272 byts.

(Ans)

3/(ii)

Fragment offset for 7th packet:

Data per full fragment = 240 bytes

offset in 8-byte units = (fragment n - 1) x (240/8).

For 7th fragment,

offset = 6 x 30 = 180

(Ans)

3/(iii)

Given,

Total data = 2552 bytes.

Full fragments (240 data each) = 10 fragments

Remaining data = 152 byte

∴ total = 11 packets

(Ans)

Day :
Time : Date : / /

Ans to the Question No-04

R2 learns about neighbors via directly connected networks and hello messages / protocol handshakes. In first iteration of Distance Vector R2 sends its entire routing table to each neighbor.

Network 192.10.11.0/24 (R1-R2 Link) → to R1
Network 191.54.20.128/25 (R2-R3 link) → to R3
and any connected LAN routs.
So R2 sends (network, cost) entries for directly connected networks with cost 0 or 1.

Ans to the Question No-05

5/1

2001:0db8:12af:0000:0000:0000:0a20:0001
short form: 2001:db8:12af::a20:1
Type: Global Unicast
Purpose: Routable public IPV6 address for internet communication.

5/11

0000:0000:0000:0000:0000:0000:0001
short form: ::1
Type: Loopback
Purpose: Allows a device to send packets to itself for testing.

Day: _____

Time: Date: / /

Ans to the Question No-06

6(i)

Two possible reason for ping failure:

1) Default gateway misconfigured on the lab computer.
2) Firewall / ACL blocking icmp at campus border or on the internet server.

6 (ii)

Yes, admin can use.

1) Ping to test connectivity to internet gateway first (internal issue)
2) traceroute to see where packets stop.
3) helps identify if problem is inside on outside.

Ans to the Que No- 7

7 i(i)

Given,

Fragment offset is measured in 8 byte blocks, not bytes.

13 bits → max offset value = $2^{13}-1$ = 8191 blocks.

8191 blocks x 8 bytes/block = 65,528 bytes max offset in bytes.

Since IPV4 packet max size is 65,535 bytes this covers it.

So 13 bits are enough by scaling offset by 8.

(Ans)

Day:
Time: Date: / /

7/(11)

The Identification field (16 bits) is a unique value assigned to each original packet. All fragments of the same packet share the same Identification value so the receiver can correctly reassemble them together.

Answer to the Question No - 8

8/(1)

The PC broadcasts initially because it doesn't know any DHCP server IP address. Broadcasting ensures that any DHCP server on the local network can receive the request.

8/(11)

The PC receives a DHCP offer from a DHCP server, containing

⇒ offered IP address
⇒ Subnet mask
⇒ Default gateway
⇒ DNS server
⇒ lease time

The PC replies with a DHCP request to confirm acceptance of the offered IP.

Day:
Time: Date: / /

Ans to the Question No - 09

9/(i)

The recruiter can't access because:

⇒ The server is on private IP (10.10.5.50) behind NAT.

⇒ NAT router doesn't forward incoming traffic to that server unless port forwarding or static NAT is configured.

⇒ Simply sharing the public IP without a port mapping means incoming requests to default ports aren't forwarded to port 8080 inside.

9/(ii)

Configure port forwarding on the router:

Map Public_ip: 8080 → 10.10.5.50: 8080.

Alternatively set up a static NAT or DMZ for that private IP if needed.

Ans to the Question No - 10

IPV6's base header is fixed length which is 40 bytes with fewer fields. The processing:

⇒ No checksum in header.

⇒ No fragmentation fields in main header.

⇒ Fixed structure.

So despite larger size, IPV6 is more efficient due to streamlined design and elimination of IPV4 legacy features.

Day :

Time : Date : / /

Ans to the Question NO 11

11/(I)

Host A knows it's own ip (192.168.1.10) and Host C's IP (192.168.1.20) but doesn't know Host C's MAC.

Since they're on the same subnet, Host A will send an ARP request.

Source MAC: AA-AA-AA-AA-AA-AA

Destination MAC: FF-FF-FF-FF-FF-FF

ARP message: 'Who has 192.168.1.20? Tell 192.168.1.10'

Switches process it and forward the broadcast frame out all ports except the incoming one and also learn that AA-AA-AA-AA-AA-AA is on the port where the request came from.

11/(II)

Switches are 'plug and play' because they automatically learn MAC Addresses and build forwarding tables without manual configuration and use Spanning Tree protocol to prevent loops dynamically. NO IP configuration needed for basic layer-2 switching.