Assignment-2

CSE421

Name: Tangena Akter Prity

ID : 24141171

Sec : 23

Ans to the Q. no → 1

I. Given,

IP address : 137. 168. 210. 108

Subnet mask: 255. 255. 240. 0

Prefix = 20

Host bit = 32 − 20 = 12

No. of host $= 2^h - 2$

$= 2^{12} - 2$

$= 4096 - 2$

$= 4094$ hosts

So, The organization can support 4094 hosts.

II. subnet mask 20

block size in 3rd Octet

256 − 240 = 16

3rd octet IP = 210

16×13 = 208

Network address: 137.168. 208. 0/20 (Ans)

III. Given,

LAN A = 2000 hosts

LAN B = 480 hosts and 2 WAN links

LAN C = 350 hosts

Base Network address: 137. 168. 208. 0/20

For LAN A: $2^{11}-2$ = 2046 hosts → /21

Network: 137.168.208.0/21

For LAN B: $2^{9}-2$ = 510 hosts → /23

Network: 137.168.216.0/23

For LAN C: $2^{9}-2$ = 510 hosts → /23

Network: 137.168.218.0/23

WAN Links (2 hosts each)

$2^{2}-2$ = 2 hosts → /30

WAN1 : 137.168.220.0/30

WAN2 : 137.168.220.4/30

Ans to the Q.no → 2

I. The ISP router uses PAT (Port Address Translation) PAT maps IP and Port combinations. If same source port exists, router assigns a different external port. ~~Replies are matched using the PAT translation table.~~ Basically, ISP router checks the destination port number in the incoming reply and matches it with its PAT table to identify whether the packet belongs to device A or device B.

(iii) Device A & B use private IP addresses. 192.168.20.0/24 and ISP uses a public IP address. Private IPs are not routable on the Internet, while the public IP is globally routable and used by PAT to represent multiple internal devices.

Ans to the Q. no → 3

I. Data per fragment 830 − 30 = 800 bytes

Number of fragments : 8240 ÷ 800 = 10.3 → 11 fragments

Ans: 11 fragments

II. 10 fragments × 800 = 8000 bytes

Remaining = 8240 − 8000 = 240 bytes

Ans: 240 bytes

III. Fragment offset unit = 8 bytes

Offset = data sent ÷ 8

Data before 7th fragment: 6 × 800 = 4800 bytes

offset: $\frac{4800}{8} = 600$

Ans: Fragment offset = 600

(iv) If the DF bit is set, the router drops the packet and sends an ICMP error message indicating fragmentation is required.

Ans to the Q.no→4

I. 2001:db8:0001:0:100:0

Specified blocks = 2+4 = 6

2 blocks of 0000

Ans: 2001:0db8:0000:0000:0001:0000:0100:0000

II. 0:1::

Specified blocks = 2

:: = 3 blocks of 0000

Ans: 0000:0001:0000:0000:0000:0000:0000:0000

III. 2002:C6::DB80:0:0

Specified blocks = 2+3 = 5

:: = 3 blocks of 0000

Ans: 2002:00c6:0000:0000:0000:db80:0000:0000

Ans to the Q.no→5

I. IP route 172.31.10.0 255.255.255.0 192.168.10.1

Problem: This is a next-hop-only static route causes recursive lookup. Router must resolve how to reach 192.168.10.1 then forward.

Improvement: use exit-interface or fully specified route. IP route 172.31.10.0 255.255.255.0 s0/0 directly attached or IP route 172.31.10.0 255.255.255.0 s0/0 192.168.10.1 fully specified.

(II) R2→ Pointing to R1 (R2 is a stub toward outside networks).

R1→ pointing to ISP (R1's path to outside is via ISP)

Justification: Default route is used on routers that have one main exit path to reach all unknown networks.

Ans to the Q.no→6

(I) When device D sends an ARP request for the MAC address of device, A, the request is sent as a broadcast frame. Therefore, switches S1, S2 and S3 receive the frame and flood it out all ports except the incoming port.

However, routers R1 and R2 do not forwoard the ARP request because routers never forward layer2 broadcast frames, so the frame is dropped at the routers interfaces and does not reach S4 or device F. As a result, devices beyond the routers, such as those connected to S4 will not receive the ARP request.

(ii). After device A sends the ARP reply, switches update their MAC address tables by learning the source MAC address and incoming port. Switch S1 learns the MAC address of D on port f2 and the MAC address of A on port f0. Switch S3 learns the MAC address of D on port f1 and the MAC address of A on port f2.

Ans to the Q.no:7

The hop limit field in the IPV6 header is used to limit the lifetime of a packet in the network and to prevent packets from looping endlesly due to routing errors. Each time an IPV6 packet passes through a router, the router decrements the hop limit value by one. When the hop limit value becomes zero, the packet is discarded by the router, ensuring that packets do not circulate indefinitely in the network. This mechanism guarantees a finite packet lifetime and also assists in network diagnostics, such as traceroute operations.

In IPV4, the field that performs the same function is called Time to live (TTL). Like hop limit, the TTL field is decreased by one at every hop and when it reaches zero, the packet is dropped. This ensures finite packet lifetime and helps in troubleshooting tools like traceroute.

Ans to the Q.no → 8

We call link state routing protocol a global routing because in link state, each other builds a complete topology map via LSP flooding then each runs Dijkstra (SPF) using global info. It is more efficient because faster convergence, no periodic full-table broadcasts like DV, less chance of DV problems. Because, slow convergence.

Ans to the the Q.no→9

(I) No DHCP requests from any PCs of LAN1 are reaching the DHCP server. Because DHCP request are broadcasts and routers do not forward broadcasts from LAN1 to LAN2. Therefore, the DHCP discover messages are dropped at the router interface. the solution is to configure the router connected to LAN1 as a DHCP relay agent using the ip helper-address command, which forwards DHCP requests as unicast packets to the DHCP server.

(ii) For the renewal of a leased IP address, two DHCP messages are exchanged between the client and the DHCP servers. The client sends a DHCP request message to request the extention of the lease and the DHCP server replies with a DHCP ack message to confirm and renew the lease.

Ans to the Q.no→10

(i) 98:CC:12:23:40:BB

To identify whether it is unicast or multicast, we check the least significant bit of the first octet. The first octet is 98. In binary $\overset{98\rightarrow}{\uparrow}$ 10011000. where the last bit is 0. so, therefore this

MAC address represents a unicast address, which is basically used to communicate with a single device on the network.
So, given address is unicast address.

(ii) The MAC address of a packet changes at every hop because MAC addresses are used for local (link-layer) delivery between directly connected devices. Each router removes the incoming frame and creates a new frame with its own MAC address as the source and the next hop is MAC address as destination. However, the IP address does not change because IP addresses are used for end-to-end communication at the network layer to identify the source and destination devices across different networks.

Ans to the Q.no→ 11

When a device in a network wants to send a packet to another device located in a different network, it can not directly obtain the MAC address of the destination device because ARP works only within the local network. Therefore, at the initial stage, the sending device sends an ARP request for the MAC address of its default gateway (first hop router), not for the remote destination device. The sending device then encapsulates the IP packet in a frame addressed to the MAC address of the default gateway, which forwards the packet towards the destination network.

The IP address of the device that needs to be ARPed for the default gateway which is obtained from the device's IP configuration, which is typically assigned by a DHCP server or configured manually by a network administrator. This default gateway address tells the device where to send packets destined for remote networks.