Assignment - 02

Name: MD. Mehanab Hossain Alvy

ID: 24241164

Section: e2

Course: CSE421

Date: 06.01.26

Ans. to the ques. no - 01

(I)

IP: 3.12.66.26/19

Subnet mask: 255.255.224.0

66 in binary: 01000010

Mask: 11100000

After doing AND: 01000000

∴ Network Address: 3.12.64.0/19

(II)

1. R2 LAN (1000 Hosts): $2^{10} = 1024$, requires /22

Subnet: 3.12.64.0/22

range: 3.12.64.0 – 3.12.67.255

2. SW (509 Hosts): $2^9 = 512$ address. Requires /23

Start IP: 3.12.68.0

Subnet: 3.12.68.0/23

Range: 3.12.68.0 – 3.12.69.255

3. R4 LAN (128 Hosts): 128 + 2 + 1 = 131. Needs $2^8 = 256$.
Requires /24

Start IP: 3.12.70.0

Subnet: 3.12.70.0/24

Range: 3.12.70.0 – 3.12.70.255

4. WAN : As 3 links. 2 IP need's for each. requires /30.

R1-R2: 3.12.71.0/30

R2-R3: 3.12.71.4/30

R3-R4: 3.12.71.8/30

(iii)

For R2 LAN,

Block size (/22): 1024 addresses

Used: 1000+1+2 = 1003

Wasted: 1024 - 1003 = 21 addresses.

Ans. to the ques. no - 02

(i)

Directly connected networks are identified by the Protocol code 'C' or 'L'. The point to an exit interface rather than a next-hop IP address and typically have a metric/cost of 0.

(ii)

Recursive Default Static Route on R2. R2 needs to reach the ISP via R1. The Next Hop is R1's interface IP. Command: ip route 0.0.0.0. 0.0.0.0. 192.10.11.2

(iii)

Floating Default Static Route on R2 a floating route acts as a backup, so it requires a higher AD than the primary route. Directly Attached means using the exit interface. R2 connected to R3 via S1/0/1.

Command: ip route 0.0.0.0. 0.0.0.0. S1/0/1 50

(iv)

The value inside the brackets represents AD. An AD of 40 indicates the trustworthiness of the route source and Metric of 0 indicates the cost to reach the destination.

(v)

A directly attached static route is better/faster because it resolves immediately to an exit interface in a single lookup. A recursive route requires the router to perform multiple lookups: first to find the route to the destination and second to resolve the next-hop IP to an exit interface.

Ans. to the ques. no-03

(i)

Header = 42 bytes

Payload = 362 - 42 = 320 bytes

Since 320 is divisible by 8, this is the Max Data payload.

MTU (x) = Payload + Header = 320 + 42 = 362 bytes.

(ii)

Before 5th packet, Total data = 4 x 320 = 1280 bytes

$\therefore$ offset = $\frac{1280}{8} = 160$

(iii)

Total Payload needed = 4584 - 42 = 4542 bytes

Max payload per fragment = 320 bytes

Calculation : $\frac{4542}{320} = 14.19$

So, total fragments : 14 + 1 = 15

Ans. to the ques. no-04

(i) After using Dijkstra's Shortest Path First.

Diagram: R3 → R2 → R1 → R4 → PCC

1. Iter 0: R3 knows itself.
2. Iter 1: R3 adds closest neighbor R2.
3. Iter 2: R3 adds R2's neighbor R1.
4. Iter 3: R3 adds R1's neighbor R4

So, 3 Iterations.

(ii)

Detecting Lost connection in Link State routing, routers exchange periodic Hello packets. If R1 stops receiving Hellos from R4 for a specific time, R1 declares the neighbor dead. R1 then floods a Link state Update to all other routers to update their topology maps.

Ans. to the ques. no-05

(i)

Given: 2001:0db8:12af:1::0:3

Expanded: 2001:0db8:12af:0001:0000:0000:0000:0003

(ii)

Type: Global Unicast Address

Purpose: These addresses are globally unique and routable on the public Internet, similar to IPv4 public addresses, allowing communication between a host and any other host on the internet.

Ans. to the ques. no-06

For security to prevent network reconnaissance and DoS attacks. Like, An admin blocks Echo Requests so that attackers can't scan the network IP range to find active targets to attack.

Ans. to the ques. no-07

Because it determines the smallest Maximum Transmission Unit allowed along the entire path from source to destination. We need it to prevent fragmentation, which increases CPU Overhead on routers/hosts and results in total data loss if a single fragment is dropped during transmission.

Ans. to the ques. no-08

DHCP request the client broadcasts the DHCP request to inform all available DHCP servers of its decision. This ensures that the servers whose offers were rejected can release those reserved IP addresses back into their available pool. When renewing, the packet is unicast because the client already has an assigned IP and knows the specific server's address.

Ans. to the ques. no - 09

(i)

Rajib is likely behind a NAT router. His game server is hosted on a private IP address, which is not normally on visible from the public Internet where Saif is located.

(ii)

Rajib must configure Port Forwarding on his router. This forwards incoming traffic from the router's public IP on the specific game port to Rajib's local private IP address.

Ans. to the ques. no - 10

(i)

This is IPV6 addressing, the exception to the no duplicate rule is made here because Anycast explicitly allows multiple devices to share the same IP address, with the network routing traffic to the topologically "nearest" servers.

(11)

It improves reliability and performance, while also mitigating DDoS attacks by localizing traffic.

Ans. to the ques. no - 11

(i)

The destination MAC will be that of the Default Gateway, not Host Y. Host X determines Host Y is on a different network via subnet masking. X checks its ARP table for the Gateway's MAC; if missing, it broadcast an ARP Request and the router replies with it's MAC.

(ii)

Switches as self-learning: Switches are self-learning because they automatically build their MAC address table by inspecting the source MAC address of incoming frames. When Host X sends a frame to the router, switch S1 reads the source MAC and records that "MAC ... is connected to port -". Future traffic destined for X is sent only to F1.