Date:

S S M T W T F

Ans to the ques no- 01

Abdullah Al Mazid Zomader
24241189

Fall 2024 - Set A

I) Subnet Mask

Max host = 16382

So, $2^h - 2 = 16382 \Rightarrow h = 14$ host bit

prefix = 32 - 14 = 18

∴ Subnet Mask = 255.255.192.0

II) Network Address

With /18, the 3rd octet block size is 256 - 192 = 64, so range are:

0 - 63, 64 - 127, 128 - 191, 192 - 255

Given broadcast is 42.1.63.255, its the end of 0 - 63 block. so:

Network address = 42.1.0.0

III)

LANA : 2000 hosts → needs $2^{11} - 2 = 2046$ → /21

LANB : 1022 hosts → needs $2^{10} - 2 = 1022$ → /22

LANC : 512 hosts → needs $2^{10} - 2 = 1022$ → /22

WAN links (2) : typically point - to - point /30 (2 usable hosts)

Allocate from the start of 421.1.0.0/18:

Subnet	Needed Host	Prefix/Mask	Network Add	Broadcast
LANA	2000	/21	421.0.0/21	42.1.7.255
LANB	1022	/22	42.1.8.0/22	42.1.11.255
LANC	512	/22	42.1.12.0/22	42.1.15.255
WAN1	2	/30	42.1.16.0/30	42.1.16.3
WAN 2	2	/30	42.1.16.4/30	42.1.16.7

Date

S S M T W T

Ans to the ques no-02

I) This is PAT, also called NAT overload

Reasons:

① Inside network has 100+ user on the private block 192.168.50.0/24

(II) The company only has 5 public IPs

(III) Yet, all employees can access the internet simultaneously.

II) Giving the director's better internet, requires changing the edge policy, not the addressing.

Best practice is to adjust QOS and bandwidth guarantees for directors.

On the router, identify directors' polic devices & apply QOS policies:

① Priority queuing and low latency queue for their traffic.

② Or a guaranteed minimum bandwidth (reserved rate)

③ And optionally rate limit non critical traffic for everyone else during office time.

Date:

Ans to the ques no-03

First compute the payload size and the maximum payload per fragment:

→ Total Length = 5086 bytes

→ IPV4 header = 20 byte

→ original data = 5086 - 20 = 5066 bytes

Link can carry max 1244 bytes per IP packet (includes header), so per fragment:

→ Max data per fragement = 1244 - 20 = 1224 bytes.

→ full fragment size = $\frac{1224}{8}$ = 153

i) No of fragments created:

1224 x 4 = 4896 bytes

Remaining = 5066 - 4896 = 170 bytes

∴ So fragments = 4 full + 1 last = 5 fragments

ii) Fragment size of the last packet:

∴ Last fragment data = 170 data bytes

∴ Last fragment total Length = header + data = 20 + 170 = 190 bytes

iii) Fragment offset of the 5th fragment:

offset = $\frac{4896}{8}$ = 612 Ans

Date

iv) Significance of the Identification field:

The Identification (5656) value is copied into every fragement of the original packet.

At the destination, IP uses

Source IP, Destination IP, Protocol, Identification to group fragments that belong to the same original datagram, so it can reassemble them correctly.

v) ~~Also~~ DF = 1 means 'Don't Fragment'

Since 5086 byte exceeds the link's 1244 byte limit, the router can't forward it without fragmentation. So, it will:

→ Drop packet.

→ Send an ICMP Destination Unreachable - Fragmentation Needed back to the sender, enabling MTU discovery.

Date

S S M T W T F

Ans to the ques no 05

→ R_2 and R_3 will send hello packets

→ R_1 will also sends hello packet, but only on its Link-State - facing interfaces.

→ R1 on its DV interface will periodically sents DV updates

→ R4 and ISP router will periodically sends DV updates.

Why insufficient:

1. Updates are sent even when nothing is changed.
2. Often include many routes.
3. Leads to slower convergence, compared to link state's event driven flooding.

Ans to the ques no - 06

i) fe80:: 1c35:67ab:3f9c:d81e

↳ Expanded = fe80:0000:0000:0000:1c35:67ab:3f9c:d81e

ii) 2607:0:0:805::

↳ Expanded = 2607:0000:0000:0805:0000:0000:0000:0000

iii) fd00:abc:1234:5678::1

↳ Expanded = fd00:0abc:1234:5678:0000:0000:0000:0001

Date

Ans to the ques no-08

1) Two solutions:

i. Configure DHCP relay on the router/L3 interface of the new subnet, pointing to the main office DHCP server's IP. This forward DHCP request as unicast to the relay.

ii. Deploy a local DHCP server in the remote subnet and scope it for that subnet

Ans to the ques no-09

Use traceroute to pinpoint where the path to the external application fails.

→ Shows the hop-to-hop path (each router/L3 device) from the client/ISP edge towards the destination.

→ For each hop it gives:

1. The IP/address of the router at that hop
2. The round-trip-time measurement.
3. Where hop starts timing out/returning unreachable.

→ That lets the agent identify whether the break is:

1. Inside the client's ISP access/aggregation network
2. At an upstream/transit provider
3. Near the destination hosting network
4. or potentially the destination itself.

Date :

S S M T W T F

Ans to the ques no - 6

Use Dual stack

↓

Dual stack runs IPv4 and IPv6 simultaneously on hosts/ routers/ services etc.

1. Internal IPv4 - only remains reachable via IPv4 with no translation needed

2. IPv6 collaboration work natively over IPv6

3. End systems can choose the correct protocol automatically. (usually IPV6 preferred when available, otherwise IPv4.