

1. ① Given,

Broadcast Address = 42.1.63.255

Max Hosts = 16382

$$2^n - 2 \geq \text{Hosts}$$

$2^{14} = 16384$ means insufficient for 16382 ~~hosts~~ ^{hosts}

\therefore host bits = 14

\therefore network bits = $32 - 14 = 18$

Now subnet mask : /18

1111 1111.1111 1111.1100 0000.0000 0000

255.255.192.0

② Given, 42.1.63.255 /18

block size in the 3rd Octet = $256 - 192 = 64$

63 falls in the 0-63 range.

\therefore **Network address : 42.1.0.0**

③ ~~LANA (2000) =~~

Hosts	Needs address	Network bits	Net. Add
LANA (2000)	$2^{11} = 2048$	21	42.1.0.0/21 (42.1.0.0-42.1.7.255)
LANB (1022)	$2^{10} = 1024$	22	42.1.8.0/22
LANC (512)	$2^{10} = 1024$	22	42.1.12.0/22
WAN1 (2)	/30	/30	42.1.16.0/30
WAN2 (2)	/30	/30	42.1.16.4/30

2. ① [PAT (Port Address Translation)]

The company has ^{over} 1000 employees but only a pool of 5 public IP addresses. For all employees to access the internet simultaneously, multiple private IPs must be mapped to a single public IP using different source port numbers. Standard Dynamic NAT would fail after the 5th simulation user.

② [Configure Static NAT for three directors.]

Map the private IPs of the 3 directors permanently to specific Public IPs from the pool. This ensures they always have a dedicated address and are not competing for port translation entries, guaranteeing access and speed.

3. (i) Given, Length = 5086

Header = 20

MTU = 1244

Max Payload per fragment = $1244 - 20 = 1224$ bytes

Total payload to send = $5086 - 20 = 5066$ bytes

$$\text{No. of fragments} = \frac{5066}{1224}$$

$$= 4.13 \approx \boxed{\begin{array}{l} 5 \text{ fragments} \\ 4 \text{ full} + 1 \text{ partial} \end{array}}$$

(ii) Data sent in first 4 fragments: $1224 \times 4 = 4896$ bytes

Remaining data: $5066 - 4896 = 170$ bytes

$$\boxed{\text{Last fragment size} = 170 + 20 = 190 \text{ bytes}}$$

(iii) offset of the 5th fragment = $\frac{\text{Bytes of data sent previously}}{8}$

$$= \frac{4896}{8}$$
$$= \boxed{612}$$

(iv) It uniquely identifies the group of fragments that belong to the same original IP Packet, allowing the receiving host to reassemble them correctly.

(v) The router would drop the packet and send an ICMP "Fragmentation Needed" error message back to the sender.

P.T.O.

4. (i) 192.168.96.0 255.255.255.0 192.168.10.97 2

(ii) Exit interface: S3 on R4
192.168.96.0 255.255.255.0 S3 10

5. (i) R1, R4 and ISP. Distance Vector protocols send their entire routing table to neighbors at fixed intervals. This consumes significant bandwidth and CPU processing even when there are no network changes and leads to slower convergence.

(i) R1, R2, R3. Link state protocols use Hello packets to discover neighbors and establish adjacency relationships before exchanging routing info.

6. (i) fe80:0000:0000:1e35:67ab:3f0c:d81e

(ii) 2607:0000:0000:0805:0000:0000:0000:0000

(iii) fd00:0abc:1234:5678:0000:0000:0000:0001

7. ① Source MAC = PCA's MAC address

Destination MAC = FF:FF:FF:FF:FF:FF

② PC B receives the broadcast packet, opens the ARP payload, and sees its own IP address listed in the 'target IP' field. It realizes the request is meant for itself.

③ R1 will ~~not~~ drop the packet. ARP requests are layer 2 broadcasts. Routers create broadcast boundaries and do not forward broadcasts from one subnet/interface to another.

8. ① DHCP clients use Broadcast messages (DHCP DISCOVER) to find a server. Routers do not forward broadcasts. Since the server is on a different physical subnet/network, the router blocks the request.

② 1. Configure an IP Helper Address on the router interface connected to the new subnet.
2. Install a DHCP Relay Agent on a device within the new subnet to forward requests as unicast.

9. Traceroute

It provides the list of all routers along the path to the destination and the round-trip time for each. It helps identify the exact location of the failure.

10. Dual Stack Transition Technique.

11. ① S1 takes no action.

PCB sends the frame to S2. S2 checks its MAC table and sees that PC A is reachable via the port connected to S3. S2 unicasts the frame directly to S3. It does not flood the frame to S1.

② They are called transparent because end devices are unaware of the switch's existence. The devices operate as if they are connected to the same physical wire. The switch handles the learning of addresses and forwarding of frames 'silently' in the background without requiring configuration on the PCs.