Q1

Question 1

Figure 1-1 network topology is using Internet Protocol version 4 (IPv4) addressing. Ali and you have been assigned by the company CEO to configure the company's network topology with different types of static routes. Answer the following questions to ensure successful communications between all hosts in Figure 1-1. Assume ISP router with static routing configurations have been completed.
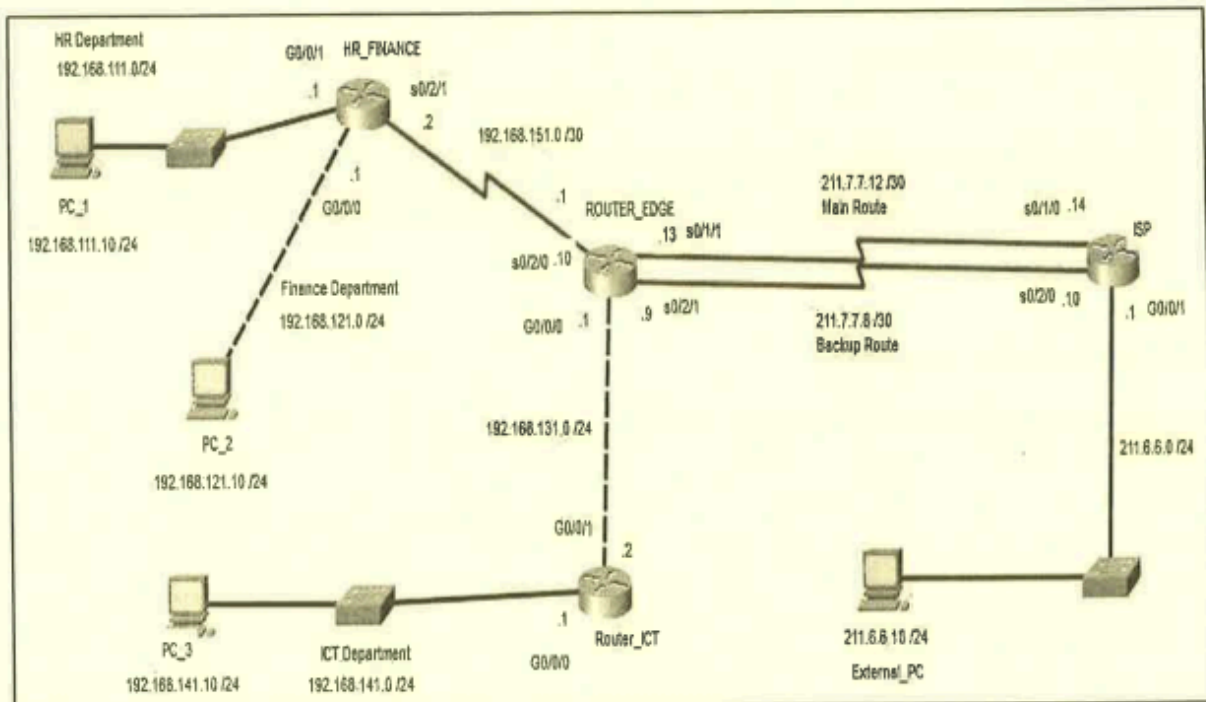

Figure 1-1: A network topology

```
ROUTER_EDGE#show ip route

Gateway of last resort is 211.7.7.14 to network 0.0.0.0

S 192.168.111.0/24 is directly connected, Serial0/2/0
S 192.168.121.0/24 [1/0] via 192.168.151.2
C 192.168.131.0/24 is directly connected, GigabitEthernet0/0/0
C 192.168.151.0/30 is directly connected, Serial0/2/0
C 211.7.7.8/30 is directly connected, Serial0/2/1
C 211.7.7.12/30 is directly connected, Serial0/1/1
```

Figure 1-2: Partial output of "show ip route"

a) In **ROUTER_EDGE**, two **standard static routes** are configured, and the partial output of show ip route command is shown in Figure 1-2. Analyse Figure 1-1 and Figure 1-2 and illustrate **TWO (2)** differences between these standard static routes.   (4 marks)

b) **(i)** In **ROUTER_EDGE**, configure **a default static route** and **a floating default static route** using the next hop IPv4 address to forward the packets to **ISP**. State your assumption in your answer. (4 marks)

ip route 0.0.0.0 0.0.0.0 211.7.7.14
ip route 0.0.0.0 0.0.0.0 211.7.7.10 10

Assume that the AD of the main route which the next hop IP address is 211.7.7.14 is 1 and is lower than AD of the floating route which the next hop IP address is 211.7.7.10 and AD is 10.

(ii) Explain the purpose of a **floating default static route** with reference to **ROUTER_EDGE** routing table. (4 marks)

c) **(i)** In **ROUTER_EDGE**, apply a **fully specified standard static route** to forward packets to **ICT Department**. (2 marks)

ip route 192.168.141.0 255.255.255.0 192.168.131.2 g0/0/0

(ii) Explain the implementation of a **fully specified standard static route** in Question 1 c) (i). (3 marks)

d) **Open Shortest Path First (OSPF)** configurations using the network command with wildcard mask based on subnet mask are to be implemented in **R1** and **R2** routers in the network topology shown in Figure 1-3. Use OSPF **process-id 666** and **area-id 0.** Propagate the default static routes in **R2** to **R1** to forward traffic to **ISP**. Assume pre-configuration of default static route in **R2** and static routes in **ISP** have been completed. Use Table 1-1 to document your answer.
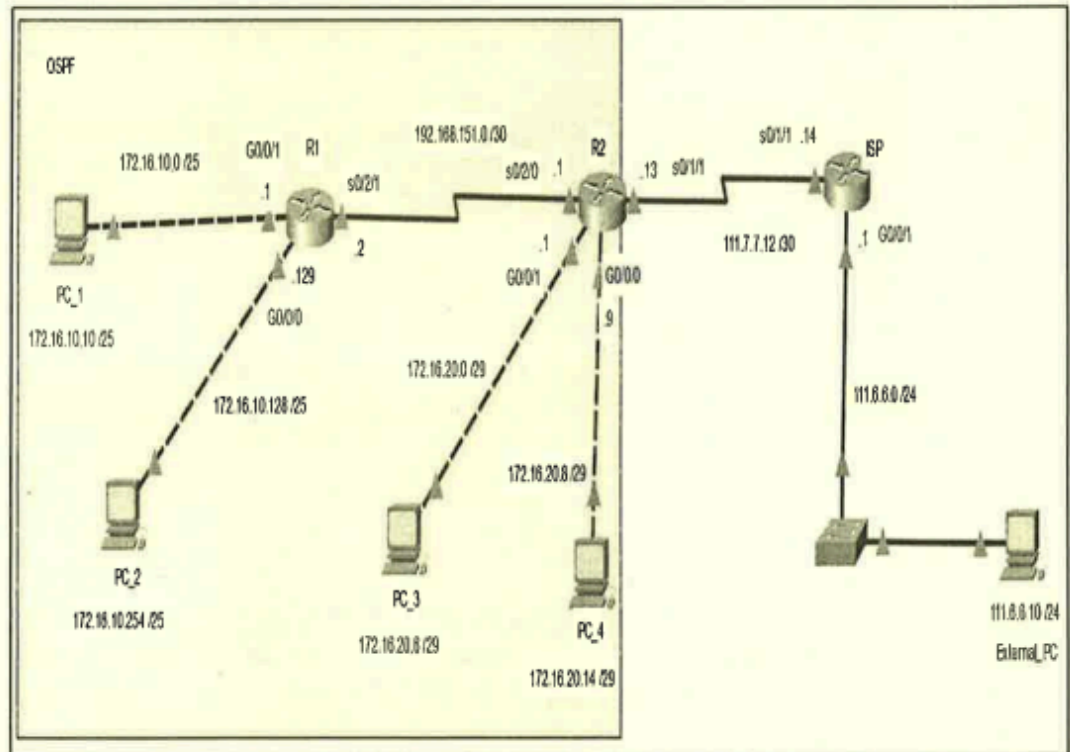

Figure 1-3: A network topology

Table 1-1: Documentation Table

Router name	Configurations

(8 marks)

[Total: 25 marks]

Router	Configuration
R1	router ospf 666 network 172.16.10.0 0.0.0.127 area 0 network 172.16.10.128 0.0.0.127 area 0 network 192.168.151.0 0.0.0.3 area 0 passive-interface g0/0/0 passive-interface g0/0/1
R2	router ospf 666

	default-information originate network 192.168.151.0 0.0.0.3 area 0 network 172.16.20.0 0.0.0.7 area 0 network 172.16.20.8 0.0.0.7 area 0 network 111.3.7.12 0.0.0.3 area 0 passive-interface g0/0/0 passive-interface g0/0/1 passive-interface s0/1/1

Q2

a)   (i)   Explain **TWO (2)** major types of Denial of Service (DoS) attacks.   (4 marks)

      (ii)   In your opinion, a DoS or a Distributed DoS Attack (DDoS) attack is more serious
              to an enterprise? Justify your answers.   (3 marks)

b)   Figure 2-1 network topology is implemented with OSPF configurations in all routers and all
      PCs can communicate with each other. Analyse the network topology to implement Access
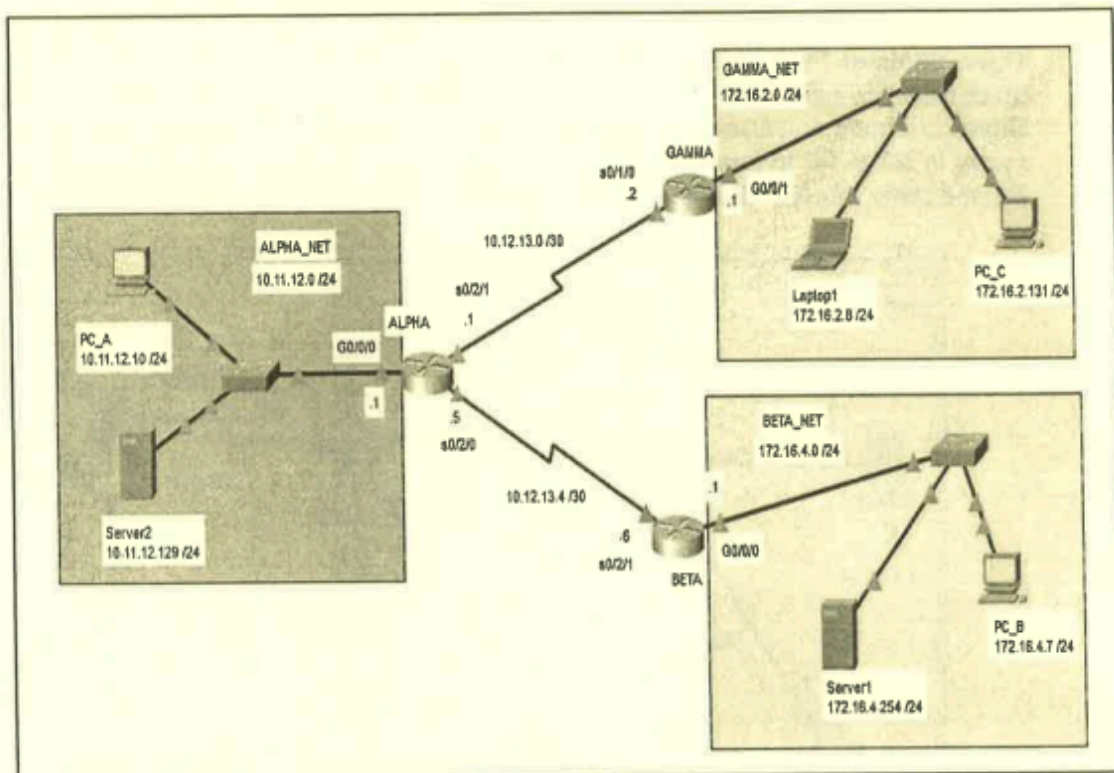   Control List (ACL) to filter the network traffic and answer the following questions.

Figure 2-1: A network topology

      (i)   Apply a standard access list named **TELNET_ACCESS** to allow only **PC_B** to telnet
             into **BETA** router. Deny all other traffic which must be explicitly written in your ACL.
             Use suitable keyword(s) in the ACL. Indicate the router, interface, and direction to
             apply the ACL.   (6 marks)

Router: BETA
ip access-list standard TELNET_ACCESS
permit host 172.16.4.7
deny any

line vty 0 15
access-class TELNET_ACCESS in

(ii) Apply an extended access list numbered 177 which will allow the second half of **GAMMA_NET** network to ping hosts with even numbered IP addresses in **ALPHA_NET**. The first half of **GAMMA_NET** network is able to access HTTP traffic on Server2. Deny all other traffic, which must be explicitly written in your ACL. Use **port number** for **services** and suitable keyword(s) in your ACL. Indicate the router, interface, and direction to apply the ACL. (12 marks)

[Total: 25 marks]

Router: GAMMA

access-list 177 permit icmp 172.16.2.128 0.0.0.127 10.11.12.0 0.0.0.254
access-list 177 permit tcp 172.16.2.0 0.0.0.127 host 10.11.12.129 eq 80
access-list 177 deny ip any any

interface g0/2/1
access-group 177 in

Q3

Question 3

OSPF and static routing protocols are configured in the respective routers in Figure 3-1 network topology and all devices are tested to be able to communicate with each other. Analyse Figure 3-1 on DHCP (Dynamic Host Configuration Protocol) and PAT (Port Address Translation) configurations in the DHCP_NAT router.
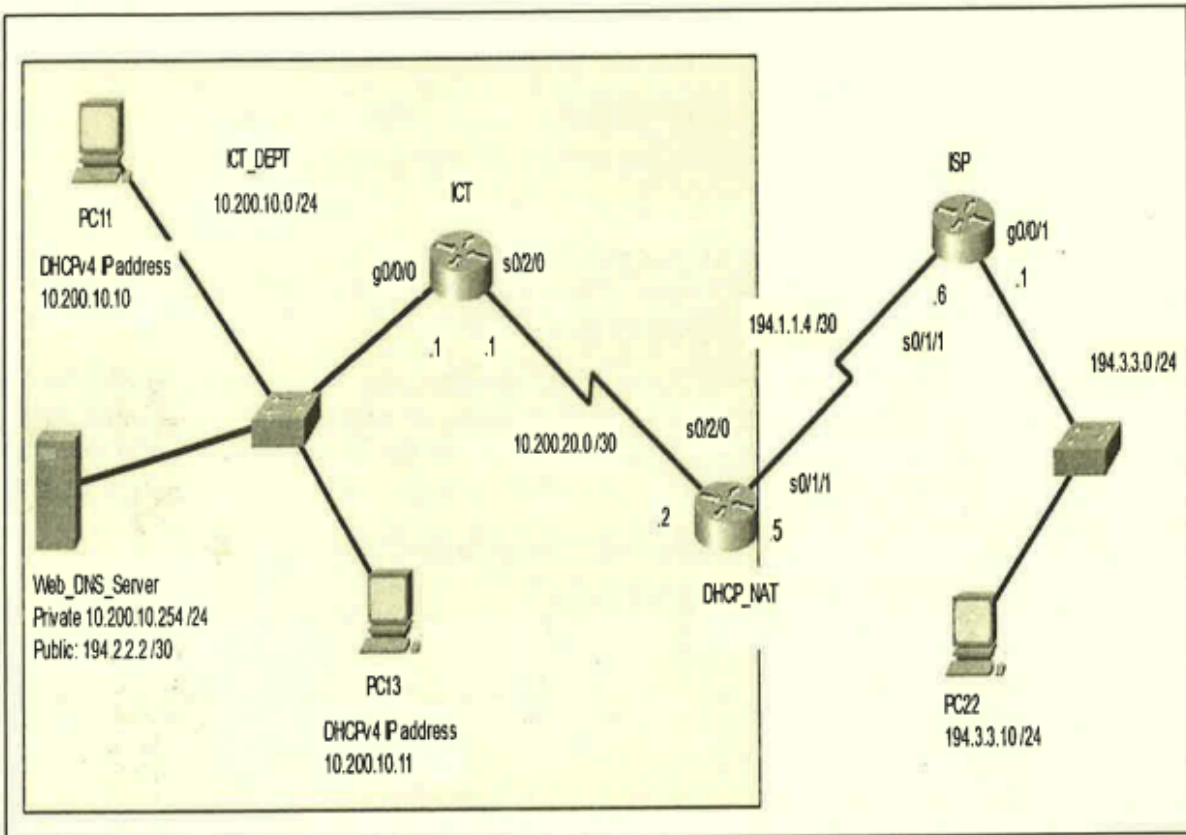

Figure 3-1: A network topology

ICT	DHCP_NAT
interface GigabitEthernet0/0/0 ip address 10.200.10.1 255.255.255. interface Serial0/2/0 ip address 10.200.20.1 255.255.255.252 : :	ip dhcp pool ICT_DEPT dns-server 10.200.10.254 interface Serial0/1/1 ip address 194.1.1.5 255.255.255.252 interface Serial0/2/0 ip address 10.200.20.2 255.255.255.252 access-list 9 permit 10.200.10.0 0.0.0.255 : :

Figure 3-2: Partial output of "show run" commands

a) **DHCP_NAT** router is configured as a DHCP server. PC11 is having a problem obtaining the IP addresses and other DHCP configurations successfully. Analyse the partial output of "show run" commands in Figure 3-2 and network topology in Figure 3-1. Use Table 3-1 to document all errors, provide the solutions/correct configurations for the respective errors and lastly justify your answers. State your assumptions in your answers. (9 marks)

Table 3-1: Documentation Table

Errors	Solutions	Justifications

Errors	Solutions	Justification

b) (i) Implement a Static NAT configuration for the **Web_DNS_Server** to be reachable from the Internet. A public address **194.2.2.2/30** is assigned to the **Web_DNS_Server** from the external network address of **194.2.2.0/30**. (7 marks)

1. nat binding
2. nat inside and outside

Static NAT
- Reserve a public address for a specific private address
- nat binding
    - ip nat inside source static [private IP address] [public IP address]
- nat inside and outside
    - interface [interface]
    - ip nat [inside / outside]

Dynamic NAT
- Will have a nat pool
- Bind the pool with access list
- Steps
    a. What is your public network
    b. What is the remain available address in your public network (as some address may use by static NAT already)
    c. Configure ACL
    d. Configure NAT pool
        - ip nat pool [name] [start public address] [end public address] netmask [subnet mask]
    e. Configure NAT binding
        - ip nat inside source list [number/name] pool [pool name]
    f. Configure NAT inside and outside

PAT (Port Address Translate)
- Will add port number behind public IP address (E.g. 194.2.2.1::1)
- Why? As port number support 0 - 65535, thus 1 public IP address can translate up to 65535 private IP address
- Configuration Methods(2)
    a. Normal configure pool
        - Same with step in dynamic NAT
        - Just NAT binding become:
            - ip nat inside source list [number/name] pool [pool name] **overload**
    b. Direct configure with interface
        - Does not configure NAT pool

- Direct use the IP address of the interface
- Step
  - Configure ACL
  - Configure NAT binding with interface
    - ip nat inside source list [name/number] interface [interface] overload
  - Configure NAT inside and outside

(ii)   Examine Figure 3-1 and Figure 3-2. Identify errors and provide solutions for PAT configurations to use the **remaining** public IP address from the external network address **194.2.2.0/30** as the pool of address. All the internal PCs should be able to ping the **Ext_PC**. Use Table 3-2 to document your answers.   (6 marks)

Table 3-2: Documentation Table

Errors	Solutions

c)   Explain NAT64.   (3 marks)

[Total: 25 marks]

Q4

<u>Question 4</u>

a)   New technologies continue to emerge in networking. Propose **TWO (2)** modern WAN (Wide Area Network) connectivity options for an enterprise and explain your answers.   (6 marks)

b)   (i)   Virtual Private Networks (VPNs) is another technology for communications on the network. Illustrate the differences between Enterprise VPNs and Service Provider VPNs.   (6 marks)

    (ii)   Compare IPsec (Internet Protocol Security) and SSL (Secure Sockets Layer) VPNs in terms of applications supported, authentication strength and connection complexity.   (6 marks)

c)   (i)   Differentiate traffic shaping and traffic policing.   (4 marks)

    (ii)   Explain a QoS (Quality of Service) method that is not suitable for VPN traffic.   (3 marks)

[Total: 25 marks]