Q1

Question 1

A network topology configured with IPv4 addressing is shown in Figure 1-1. Illustrate and configure various types of static routes by answering the following questions. Assume Internet Protocol version 4 (IPv4) addressing is configured in all devices. Assume default static routes are pre-configured in FOCS and FOET to forward traffic to HQ. In addition, **Standard static routes** and a **Floating Standard static routes** were pre-configured in **ISP** to forward packets to **FOCS_LAN1, FOCS_LAN2, FOET_LAN1** and **FOET_LAN2**.

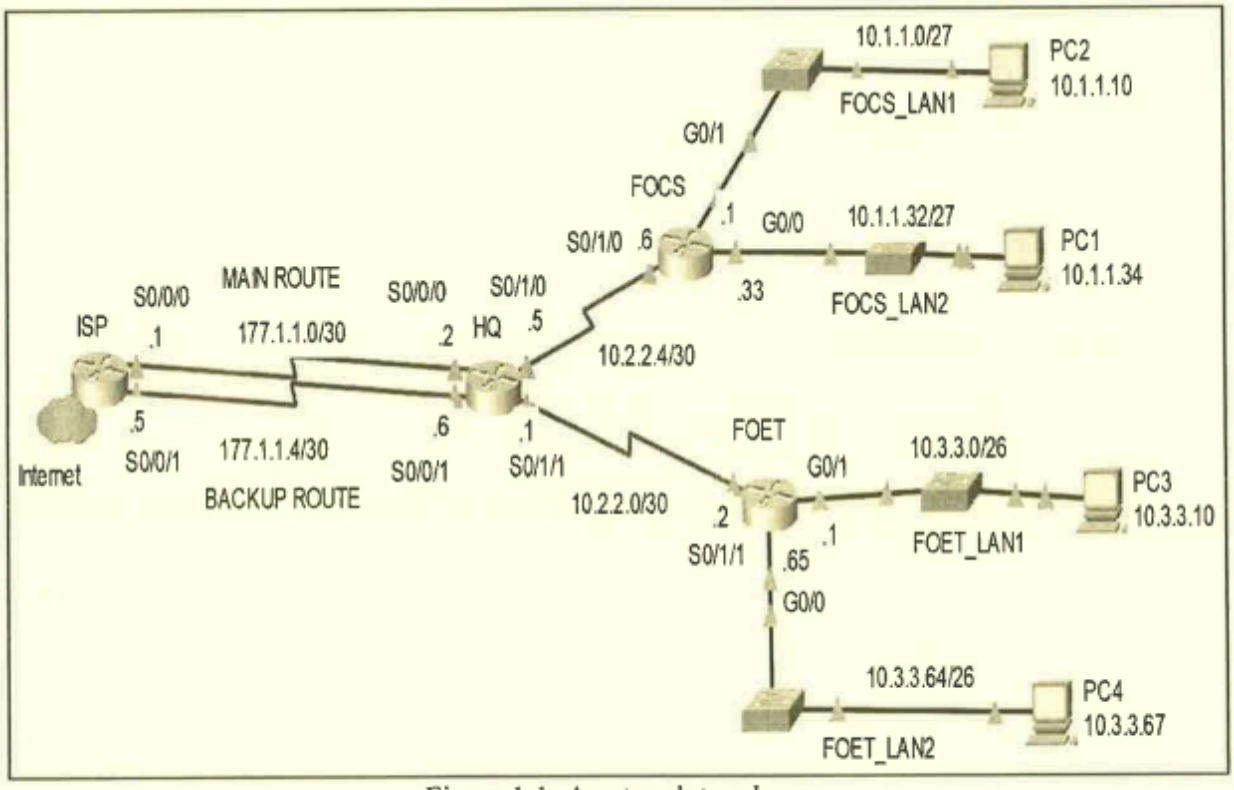

Figure 1-1: A network topology

a) (i) Configure a **Default static route** and a **Floating Default static route** in **HQ using next hop IP address** to forward traffic to the **ISP** and **Internet**. State your assumptions for the Floating Default static route. (4 marks)

ip route 0.0.0.0 0.0.0.0 177.1.1.1
ip route 0.0.0.0 0.0.0.0 177.1.1.5 10

- Assume that the Administrative Distance (AD) of the default static route with next-hop 177.1.1.1 is 1 which is lower than the ip route with next hop 177.1.1.5 and be the main route.

(ii) Configure **Standard static routes** using **next hop IP address** in **HQ** to forward packets to **FOCS_LAN1** and **FOCS_LAN2**. (3 marks)

```
ip route 10.1.1.0 255.255.255.224 10.2.2.6
ip route 10.1.1.32 255.255.255.224 10.2.2.6
```

(iii) Configure **Standard static routes** using **exit interface** in **HQ** to forward packets to **FOET_LAN1** and **FOET_LAN2**. (3 marks)

```
ip route 10.3.3.0
ip route
```

(iv) Explain the impact on **HQ** routing table search or lookup process with the implementation of different **Standard static routes** in Question 1 a) (ii) and Question 1 a) (iii). (6 marks)

b) In Figure 1-1, default static route and floating default static route to forward traffic to the **ISP** and **Internet** remained in HQ. All other static routing configured in HQ, FOCS and FOET had been removed. You are required to implement **Open Shortest Path First (OSPF)** configurations using the network command with wildcard mask based on subnet mask in **HQ** and **FOCS** only. Use OSPF **process-id 6868** and **area-id 0.** Use Table 1-1 to document your answer.

Table 1-1: Documentation Table

Router name	Configurations

(9 marks)
[Total: 25 marks]

Router Name	Configuration
HQ	router ospf 6868 default-information originate network 10.2.2.4 0.0.0.3 area 0 network 10.2.2.0 0.0.0.3 area 0 network 177.1.1.0 0.0.0.3 area 0 network 177.1.1.4 0.0.0.3 area 0 passive-interface s0/0/0 passive-interface s0/0/1
FOCS	router ospf 6868

	network 10.2.2.4 0.0.0.3 area 0 network 10.1.1.0 0.0.0.31 area 0 network 10.1.1.32 0.0.0.31 area 0 passive-interface g0/0 passive-interface g0/1

Q2

Question 2

a) (i) Organisations need to prevent various threats such as internal and external threats targeting their networks. In your opinion, which is more likely to cause significant damage to an organisation's network, internal or external threats? (3 marks)

(ii) Illustrate **TWO (2)** impact of data loss for an organisation network. (4 marks)

b) As an Associate Network Engineer, your task is to implement Access Control Lists (ACL) to filter network traffic as shown in Figure 2-1, and then answer the following questions. Assume all PCs and routers can communicate with each other.

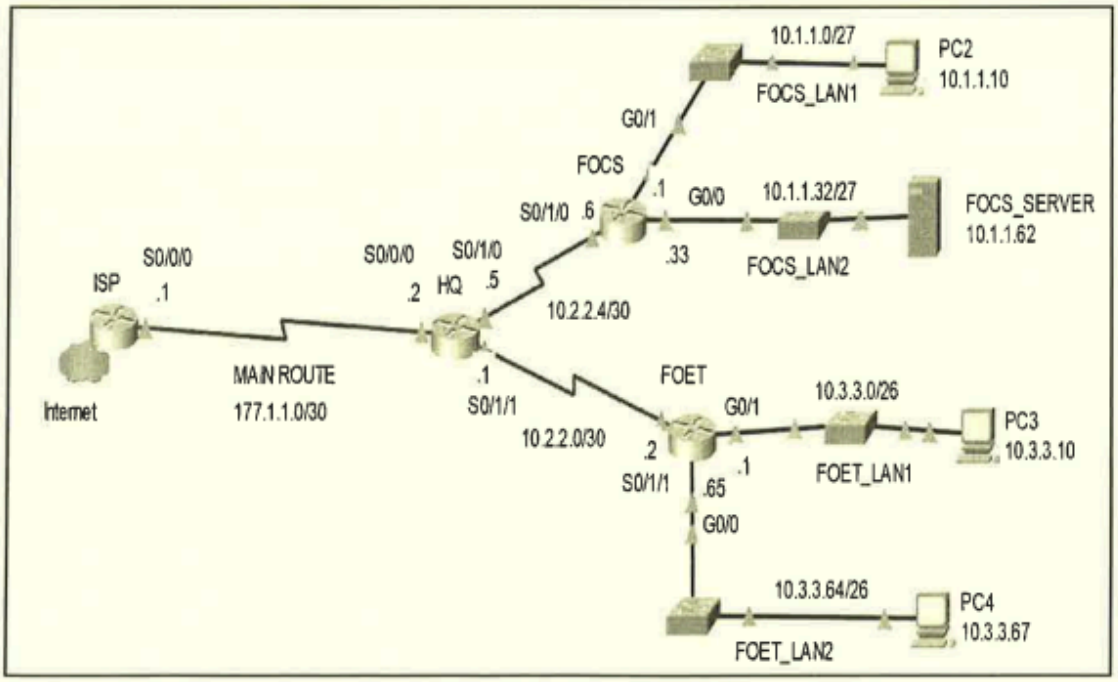

Figure 2-1: A network topology

(i) Write a standard access list named **REMOTE_LOGIN** to allow only **PC2** to telnet into **FOCS** router. Deny all other traffic, which must be explicitly written in your ACL. Use the keyword in your ACL. Indicate the **router**, **interface** and **direction** to apply the ACL. (7 marks)

Router: FOCS

```
ip access-list standard REMOTE_LOGIN
permit host 10.1.1.0
deny any

line vty 0 4
access-class REMOTE_LOGIN out
```

(ii) Write an extended access list numbered 153 to allow **FOET_LAN1** to access the **FOCS_SERVER** via **HTTPS.** Allow **FOET_LAN2** to ping **FOCS_LAN1**. Permit ospf traffic from any source to any destination. Deny all other traffic, which must be explicitly written in your ACL. Use keywords in your ACL. Use port number **443** for **HTTPS.** Indicate the **router**, **interface** and **direction** to apply the ACL efficiently. (11 marks)

[Total: 25 marks]

```
Router FOET:
access-list 153 permit tcp 10.3.3.0 0.0.0.63 host 10.1.1.62 443
access-list 153 permit icmp 10.3.3.64 0.0.0.63 10.1.1.0 0.0.0.31
access-list 153 permit ospf any any
access-list 153 deny ip any any

interface s0/1/1
access-group 153 out
```

Q3

Question 3

Analyse Figure 3-1 and Figure 3-2 on DHCP (Dynamic Host Configuration Protocol), Static NAT and PAT (Port Address Translation) configurations. OSPF and static routing protocols are configured in the respective routers.

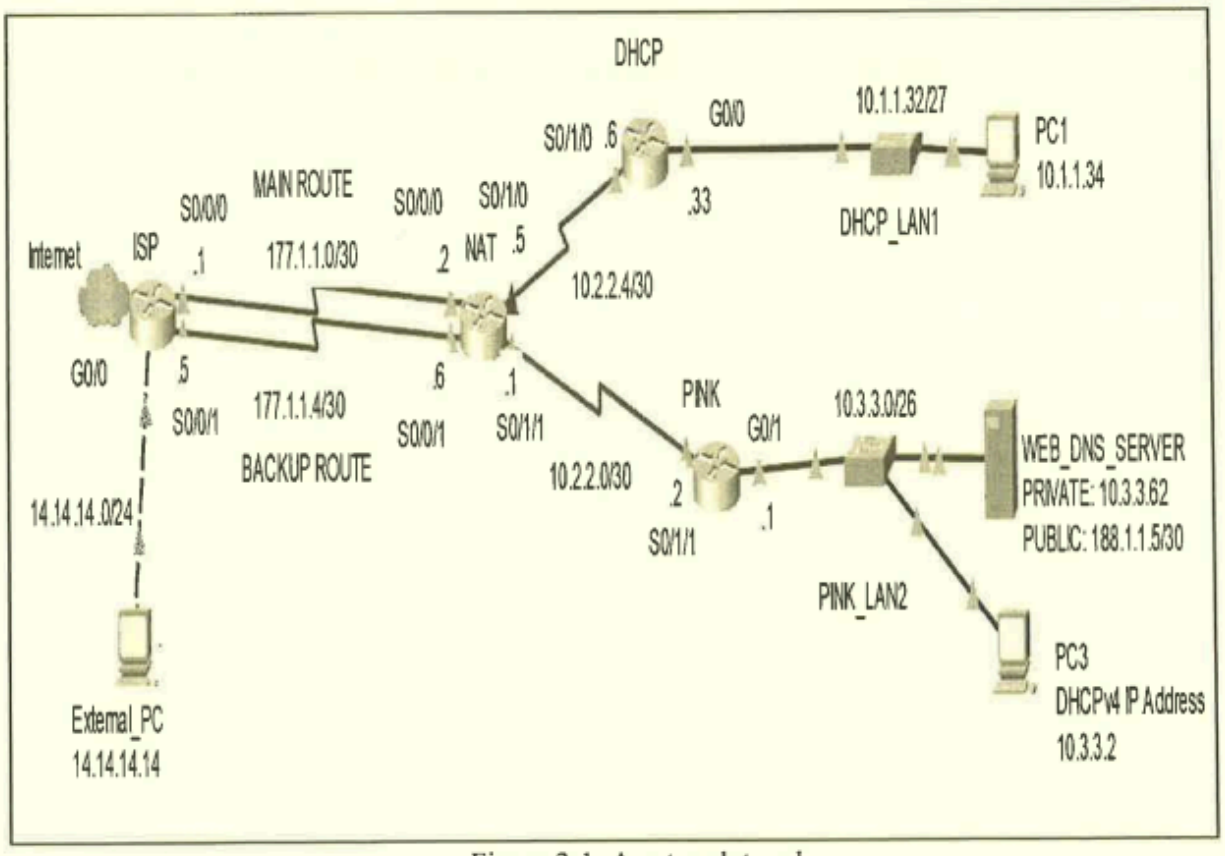

Figure 3-1: A network topology

NAT	DHCP
interface Serial0/0/0 ip address 177.1.1.2 255.255.255.252 interface Serial0/0/1 ip address 177.1.1.6 255.255.255.252 interface Serial0/1/0 ip address 10.2.2.5 255.255.255.252 interface Serial0/1/1 ip address 10.2.2.1 255.255.255.252 ip nat pool PINK 188.1.1.5 188.1.1.5 netmask 255.255.255.252	ip dhcp excluded-address 10.3.3.1 ip dhcp pool PINK interface GigabitEthernet0/0 ip address 10.1.1.33 255.255.255.224 interface Serial0/1/0 ip address 10.2.2.6 255.255.255.252
PINK	
interface GigabitEthernet0/1 ip address 10.3.3.1 255.255.255.192 interface Serial0/1/1 ip address 10.2.2.2 255.255.255.252	

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

a) **DHCP** router is configured as a DHCP server. PC3 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

b) (i) Implement **Static NAT** configurations in the respective router and apply to all the router's interfaces for the **WEB_DNS_SERVER** to be reachable from the Internet. A public address 188.1.1.5 is assigned to the **WEB_DNS_SERVER** from the external network address of **188.1.1.4/30**. (5 marks)

(ii) Assume Static NAT configurations in Question 3 b) (i) are successfully implemented. Now, identify errors and provide solutions for **PAT** configurations to use the **remaining** public IP address from the external network address **188.1.1.4/30** as the pool of address. Use 12 as the standard numbered access-list. All the internal PCs should be able to ping the **External_PC**. Use Table 3-2 to document your answers.

(11 marks)

Table 3-2: Documentation Table

Errors	**Solutions**

[Total: 25 marks]

Q4

Question 4

a) In modern WAN (Wide Area Network) connectivity, Internet-based broadband is one of the options corporations can select and implement for their communications.Illustrate **TWO (2)** wired and **TWO (2)** wireless options available for Internet-based broadband connectivity. Propose **ONE (1)** example for each option. (10 marks)

b) Explain the benefits of using VPN for transmitting network traffic. (6 marks)

c) Quality of Service (QoS) is implemented in a network using either Integrated services (IntServ) and Differentiated services (DiffServ). Describe the differences between IntServ and DiffServ. (9 marks)

[Total: 25 marks]