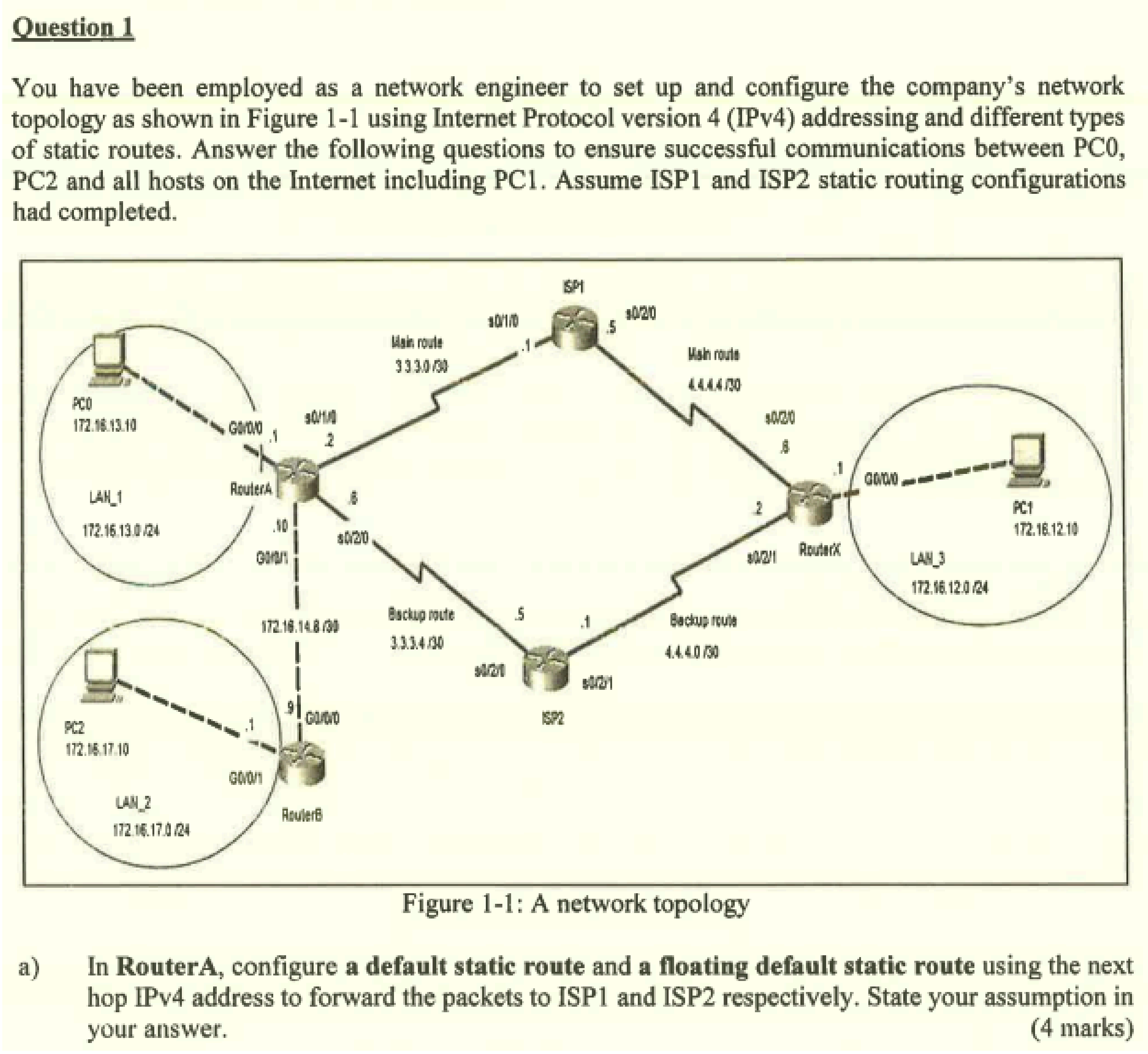
Q1



Question 1

You have been employed as a network engineer to set up and configure the company's network topology as shown in Figure 1-1 using Internet Protocol version 4 (IPv4) addressing and different types of static routes. Answer the following questions to ensure successful communications between PC0, PC2 and all hosts on the Internet including PC1. Assume ISP1 and ISP2 static routing configurations had completed.

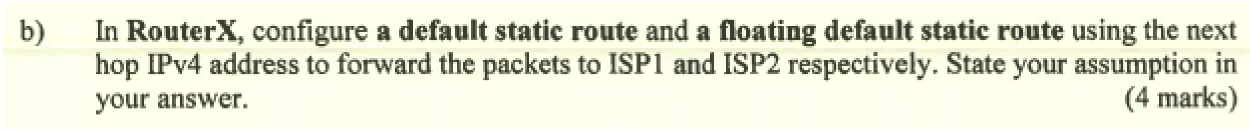
Figure 1-1: A network topology

a) In **RouterA**, configure **a default static route** and **a floating default static route** using the next hop IPv4 address to forward the packets to ISP1 and ISP2 respectively. State your assumption in your answer. (4 marks)

ISP

```
ip route 0.0.0.0 0.0.0.0 3.3.3.1
ip route 0.0.0.0 0.0.0.0 3.3.3.5 10
```

- Assume that the AD of main ip route with next hop IP address 4.4.4.6 is 1 and Therefore set the AD of the floating route with next hop address is 3.3.3.2 more higher as 10 and not become the preferred primary route.



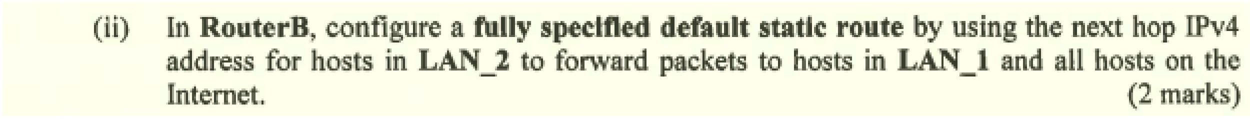
b) In **RouterX**, configure **a default static route** and **a floating default static route** using the next hop IPv4 address to forward the packets to ISP1 and ISP2 respectively. State your assumption in your answer. (4 marks)

```
ip route 0.0.0.0 0.0.0.0 4.4.4.1
ip route 0.0.0.0 0.0.0.0 4.4.4.5 10
```

- Assume the main route AD is 1. Therefore set the floating route's AD higher as 10 and not become the preferred primary routing

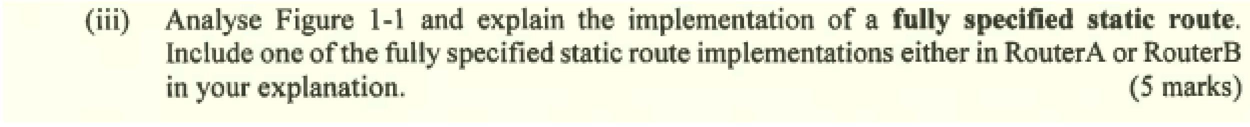
c) (i) In **RouterA,** configure a **fully specified standard static route** by using the next hop IPv4 address to forward packets to **LAN_2** network. (2 marks)

```
ip route 172.16.17.0 255.255.255.0 g0/0/0 172.16.14.9
```



(ii) In **RouterB**, configure a **fully specified default static route** by using the next hop IPv4 address for hosts in **LAN_2** to forward packets to hosts in **LAN_1** and all hosts on the Internet. (2 marks)

```
ip route
```



(iii) Analyse Figure 1-1 and explain the implementation of a **fully specified static route**. Include one of the fully specified static route implementations either in RouterA or RouterB in your explanation. (5 marks)

d) Implement **Open Shortest Path First (OSPF)** configurations using network command with wildcard mask based on subnet mask in **Router1** and **Router2** in the network topology shown in Figure 1-2. Use OSPF **process-id 888** and **area-id 0.** Propagate the default routes in **Router1** to ISP for **LAN_1** and **LAN_2** to forward the traffic to ISP. Assume pre-configuration of default route in the Router1 and static routes in ISP were completed. Use Table 1-1 to document your answer.

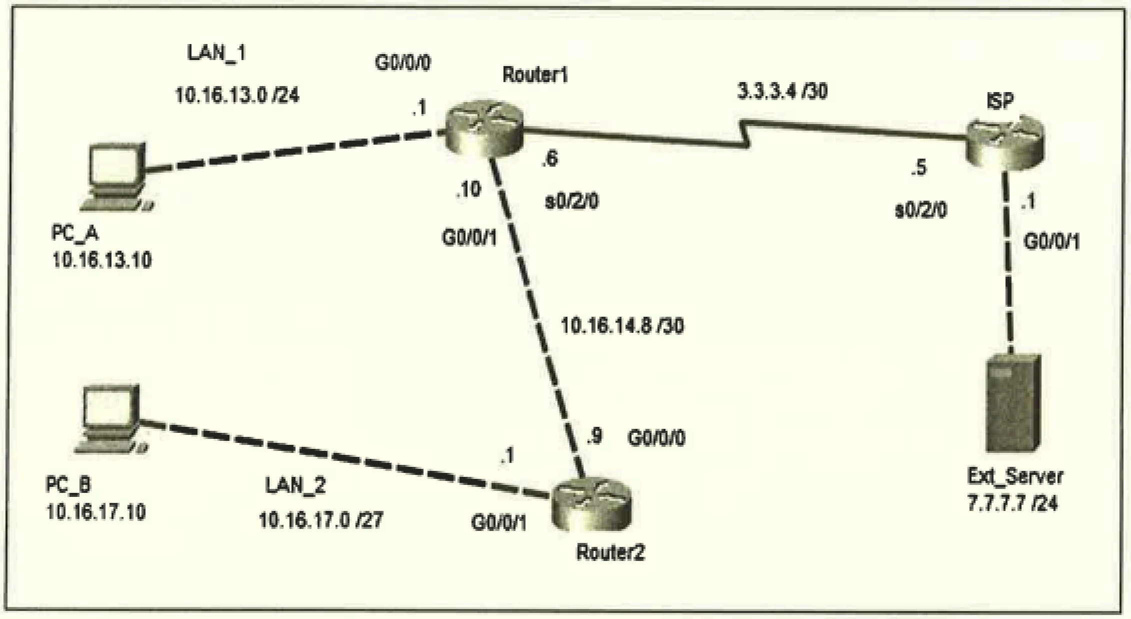


Figure 1-2: A network topology

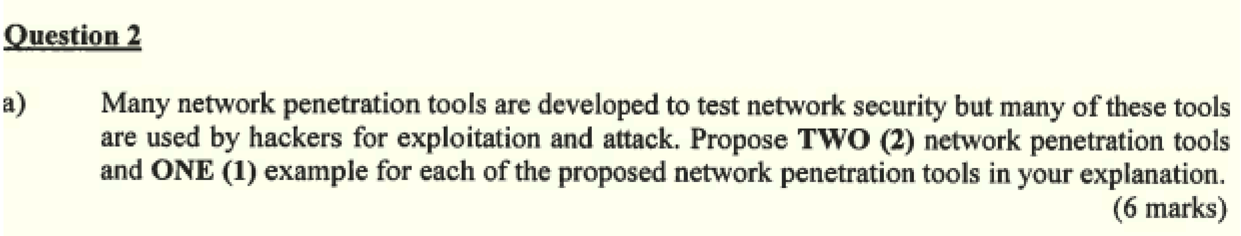
Table 1-1: Documentation Table

Router name	Configurations

(8 marks)

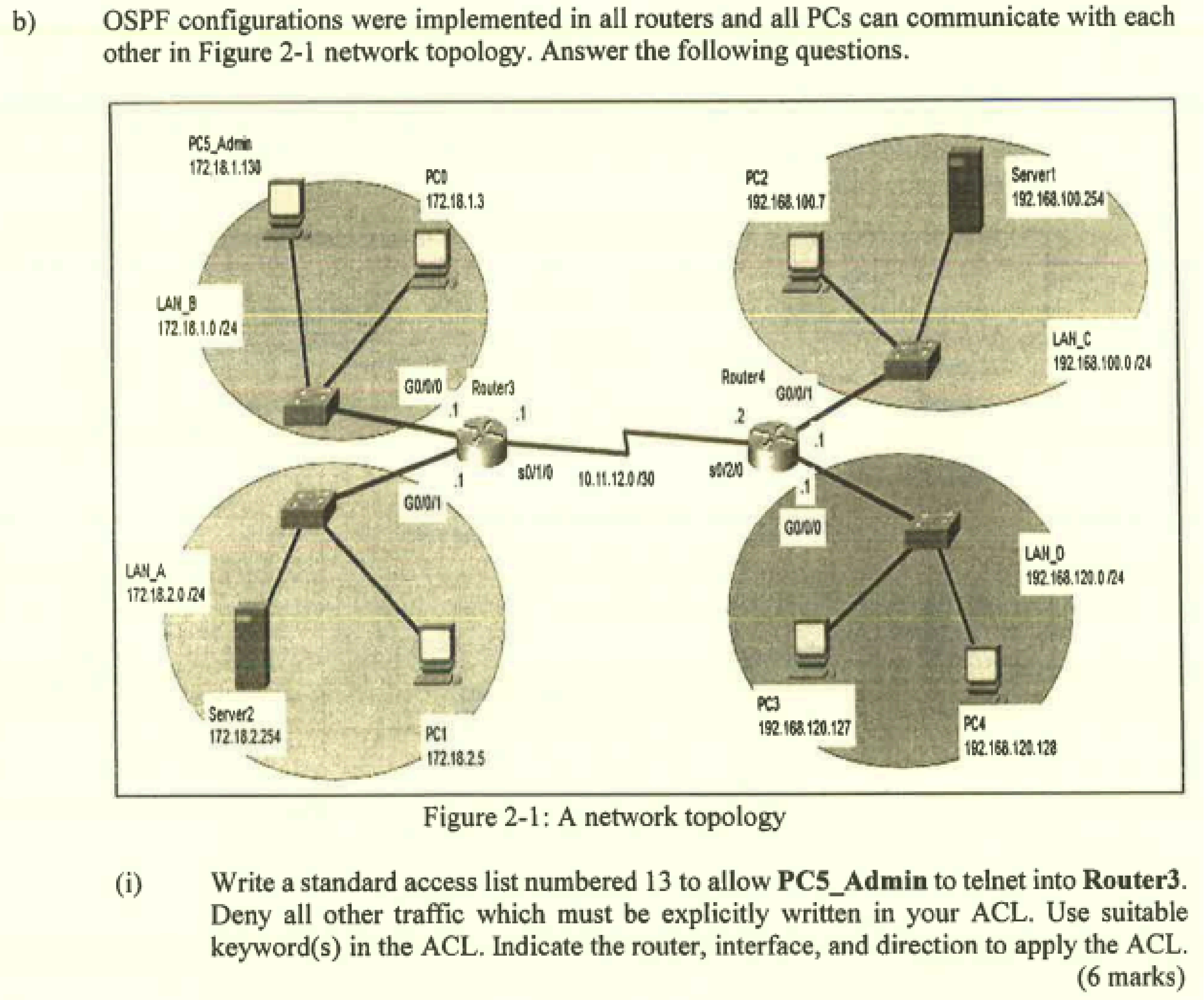
[Total: 25 marks]

Q2



Question 2

a) Many network penetration tools are developed to test network security but many of these tools are used by hackers for exploitation and attack. Propose **TWO (2)** network penetration tools and **ONE (1)** example for each of the proposed network penetration tools in your explanation. (6 marks)



b) OSPF configurations were implemented in all routers and all PCs can communicate with each other in Figure 2-1 network topology. Answer the following questions.

Figure 2-1: A network topology

(i) Write a standard access list numbered 13 to allow **PC5_Admin** to telnet into **Router3**. 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 3:
access-list 13 permit host 172.18.1.130
access-list 13 deny any
line vty 0 4

```
access-class 13 in
```

Rules

ACL (2 types)

Standard ACL (only source)

- Router most closure the destination
- [permit / deny] **host** source_IP_address
- [permit / deny] source_IP_address source_wildcard_mask
- [permit / deny] **any**

Extended ACL (source & destination)

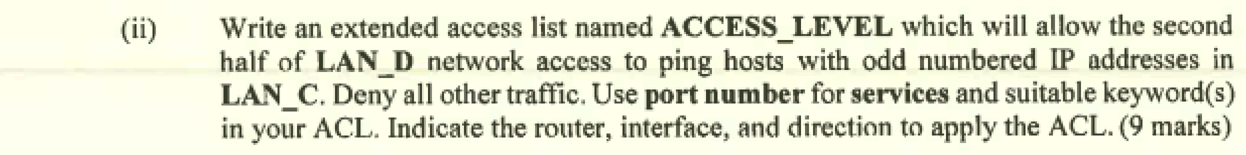
- Router most closure the source
- Formula [permit/deny] 流动的
    - [ip/icmp/**tcp**/**udp**/ospf] source_ipwm dest_ipwm [**eq** protocol]
    - [ip/icmp/tcp/udp/ospf] **host** source_IP_address dest_ipwm
    - [ip/icmp/tcp/udp/ospf] source_ipwm **host** dest_ip
    - [ip/icmp/tcp/udp/ospf] **host** source_ip **host** dest_ip
    - [ip/icmp/tcp/udp/ospf] **any any**

Named ACL

- ip access-list [standard/extended] [name]
- [permit/deny] ...

Numbered ACL

- access-list [number] [permit/deny] ...



(ii) Write an extended access list named **ACCESS_LEVEL** which will allow the second half of **LAN_D** network access to ping hosts with odd numbered IP addresses in **LAN_C**. Deny all other traffic. Use **port number** for **services** and suitable keyword(s) in your ACL. Indicate the router, interface, and direction to apply the ACL. (9 marks)

```
Router 4
ip access-list extended ACCESS_LEVEL
permit icmp 192.168.120.128 0.0.0.127 192.168.100.1 0.0.0.254
deny ip any any

interface g0/0/0
access-group ACCESS_LEVEL in
```

(iii) Differentiate applying access list on incoming and outgoing port of a router. (4 marks)

[Total: 25 marks]

Q3

Figure 3-1 shows the network topology that is set up with OSPF and static routing protocols in their respective configurations. All devices can communicate with each other. As a network associate, troubleshoot and identify the errors along with the solutions for DHCP (Dynamic Host Configuration Protocol) and PAT (Port Address Translation) configurations in the EDGE_ROUTER.

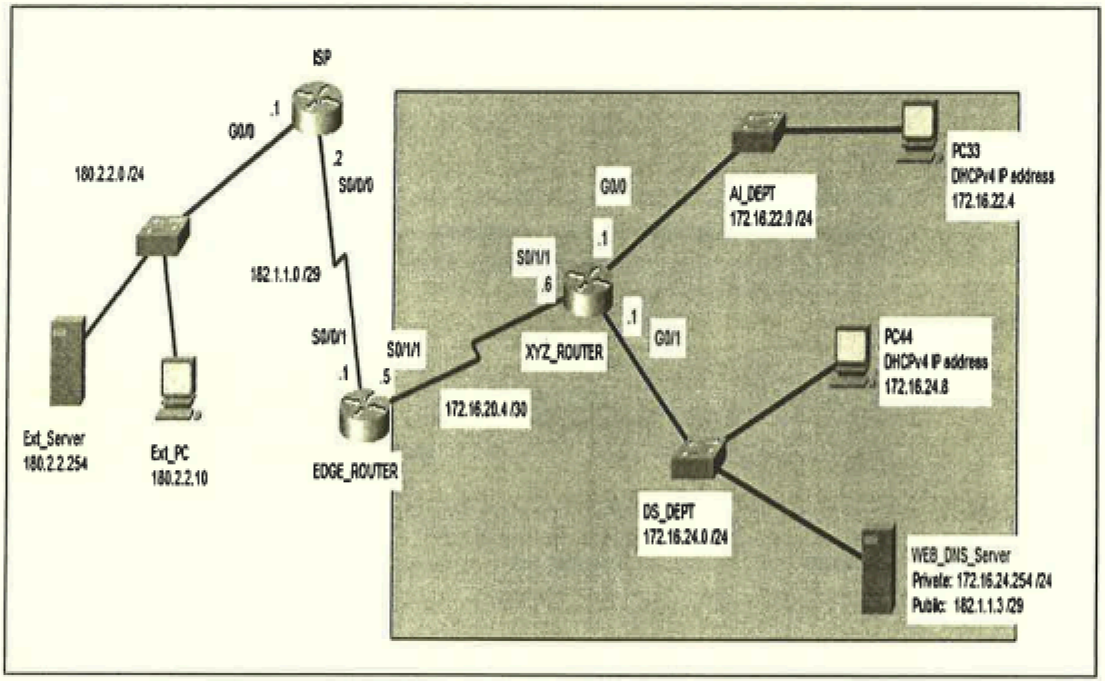
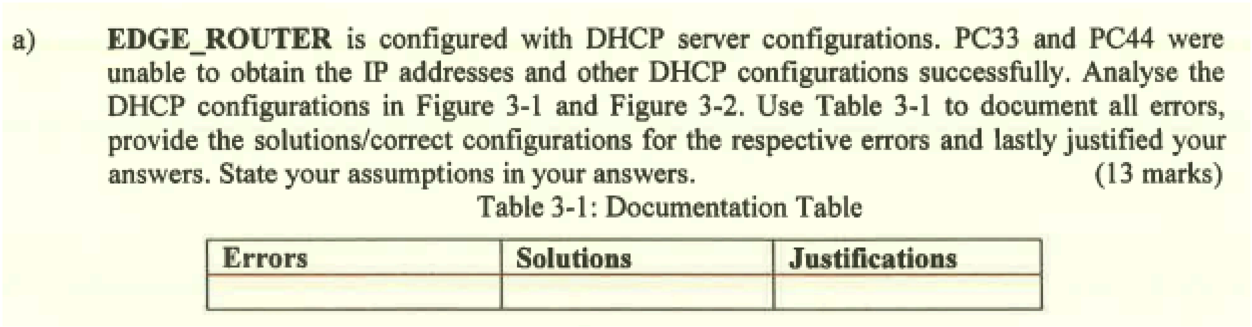


Figure 3-1: A network topology

EDGE_ROUTER	XYZ_ROUTER
ip dhcp excluded-address 172.16.24.1 172.16.24.7 ip dhcp excluded-address 172.16.24.254 ip dhcp pool DS_DEPT_DHCP network 172.16.14.0 255.255.255.0 dns-server 172.16.24.254 interface Serial0/0/1 ip address 182.1.1.1 255.255.255.248 interface Serial0/1/1 ip address 172.16.20.5 255.255.255.252 clock rate 2000000 ip nat inside source list 55 pool NAT_POOL access-list 55 permit 172.16.22.0 0.0.0.255 access-list 55 permit 172.16.24.0 0.0.0.255 :	interface GigabitEthernet0/0 ip address 172.16.22.1 255.255.255.0 interface GigabitEthernet0/1 ip address 172.16.24.1 255.255.255.0 interface Serial0/1/1 ip address 172.16.20.6 255.255.255.252 : :

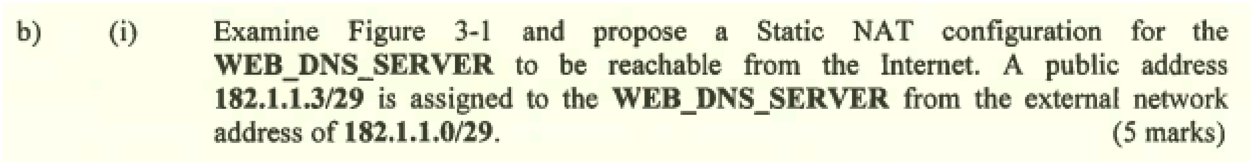
Figure 3-2: Partial output of “show run” commands



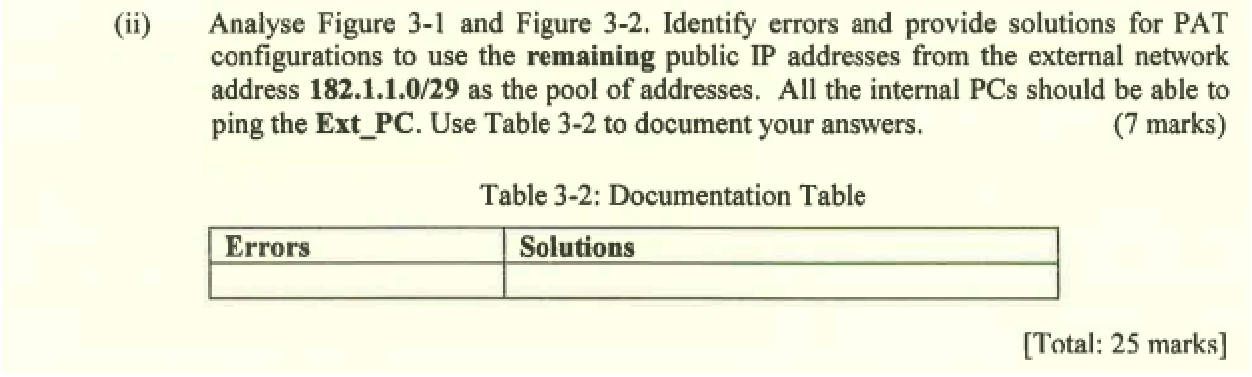
a) **EDGE_ROUTER** is configured with DHCP server configurations. PC33 and PC44 were unable to obtain the IP addresses and other DHCP configurations successfully. Analyse the DHCP configurations in Figure 3-1 and Figure 3-2. Use Table 3-1 to document all errors, provide the solutions/correct configurations for the respective errors and lastly justified your answers. State your assumptions in your answers. (13 marks)

Table 3-1: Documentation Table

Errors	Solutions	Justifications



b) (i) Examine Figure 3-1 and propose a Static NAT configuration for the **WEB_DNS_SERVER** to be reachable from the Internet. A public address **182.1.1.3/29** is assigned to the **WEB_DNS_SERVER** from the external network address of **182.1.1.0/29**. (5 marks)



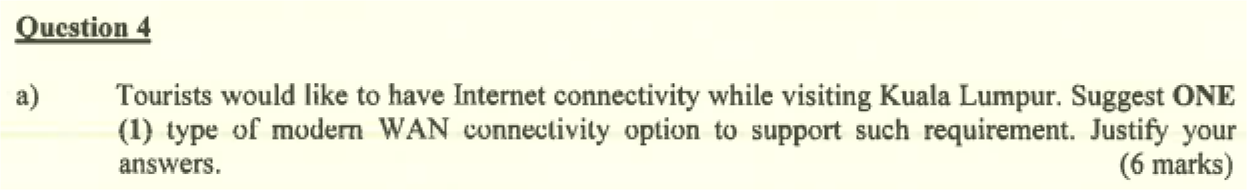
(ii) Analyse Figure 3-1 and Figure 3-2. Identify errors and provide solutions for PAT configurations to use the **remaining** public IP addresses from the external network address **182.1.1.0/29** as the pool of addresses. All the internal PCs should be able to ping the **Ext_PC**. Use Table 3-2 to document your answers. (7 marks)

Table 3-2: Documentation Table

Errors	Solutions

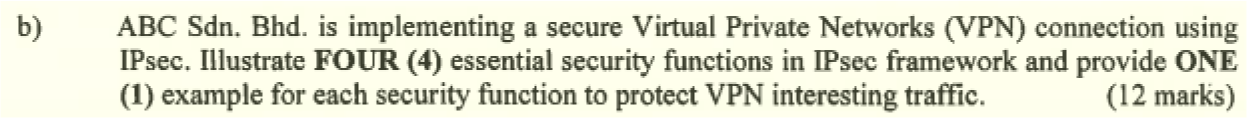
[Total: 25 marks]

Q4

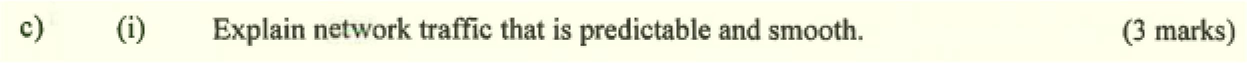


Question 4

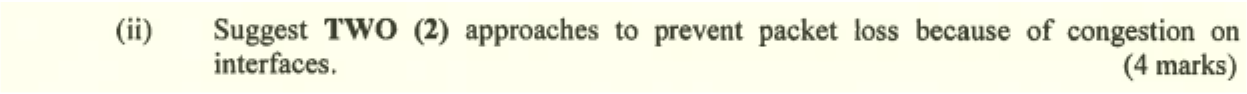
a) Tourists would like to have Internet connectivity while visiting Kuala Lumpur. Suggest **ONE (1)** type of modern WAN connectivity option to support such requirement. Justify your answers. (6 marks)



b) ABC Sdn. Bhd. is implementing a secure Virtual Private Networks (VPN) connection using IPsec. Illustrate **FOUR (4)** essential security functions in IPsec framework and provide **ONE (1)** example for each security function to protect VPN interesting traffic. (12 marks)



c) (i) Explain network traffic that is predictable and smooth. (3 marks)



(ii) Suggest **TWO (2)** approaches to prevent packet loss because of congestion on interfaces. (4 marks)