Q1

1. Based on Figure 3-1 and Figure 3-2, identify and explain the problems and provide solutions for VPN configurations.

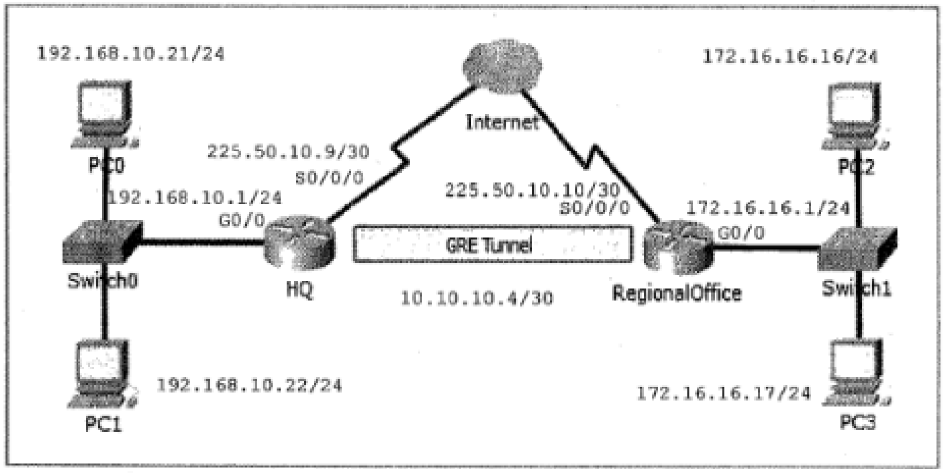
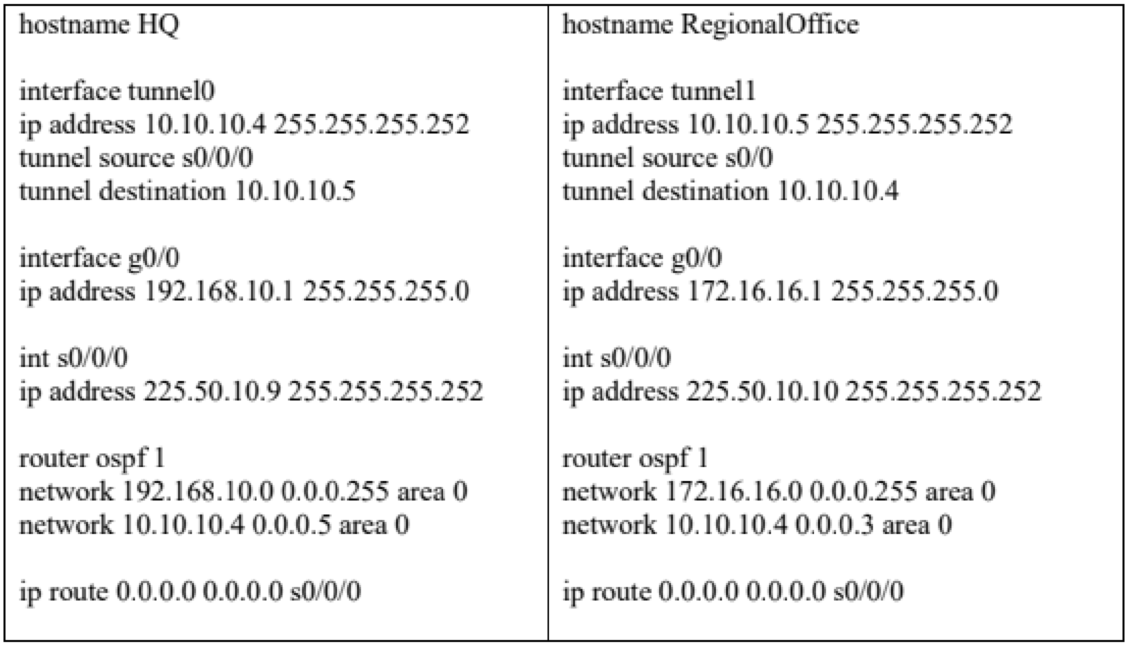


Figure 3-1: GRE Tunnel on routers HQ and RegionalOffice



hostname HQ	hostname RegionalOffice
interface tunnel0 ip address 10.10.10.4 255.255.255.252 tunnel source s0/0/0 tunnel destination 10.10.10.5	interface tunnel1 ip address 10.10.10.5 255.255.255.252 tunnel source s0/0 tunnel destination 10.10.10.4
interface g0/0 ip address 192.168.10.1 255.255.255.0	interface g0/0 ip address 172.16.16.1 255.255.255.0
int s0/0/0 ip address 225.50.10.9 255.255.255.252	int s0/0/0 ip address 225.50.10.10 255.255.255.252
router ospf 1 network 192.168.10.0 0.0.0.255 area 0 network 10.10.10.4 0.0.0.5 area 0	router ospf 1 network 172.16.16.0 0.0.0.255 area 0 network 10.10.10.4 0.0.0.3 area 0
ip route 0.0.0.0 0.0.0.0 s0/0/0	ip route 0.0.0.0 0.0.0.0 s0/0/0

Figure 3-2 GRE configurations on router HQ and RegionalOffice

IP address of HQ interface tunnel0 configure wrongly. 10.10.10.4 is network.	*configure correct IP address by command* *int tunnel0* *ip address 10.10.10.6 255.255.255.252*

Tunnel destination of HQ interface tunnel0 configured wrongly. It must be a real physical interface facing the public network.	Configure the tunnel destination correctly by command interface tunnel0 no tunnel dest tunnel dest 225.50.10.10
Wildcard mask of network 10.10.10.4 in HQ router ospf configure wrongly. /30 is 0.0.0.3	Configure the wildcard mask correctly by command router ospf 1 no network 10.10.10.4 0.0.0.5 network 10.10.10.4 0.0.0.3
The interface tunnel of Regional Office configure wrongly, should be same with HQ	Configure the interface tunnel correctly by command no interface tunnel1 interface tunnel0 ip add 10.10.10.5 255.255.255.252 tunnel source s0/0 tunnel destination 10.10.10.4
Tunnel source of Regional Office in interface tunnel0 configure wrongly	Configure the tunnel source correctly by command int tunnel0 no tunnel source tunnel source s0/0/0
Tunnel destination of Regional Office in interface tunnel configure wrongly. It must be real physical interface facing the public network.	Configure the tunnel destination correctly by command int tunnel0 no tunnel dest tunnel dest 225.25.10.9

Q2

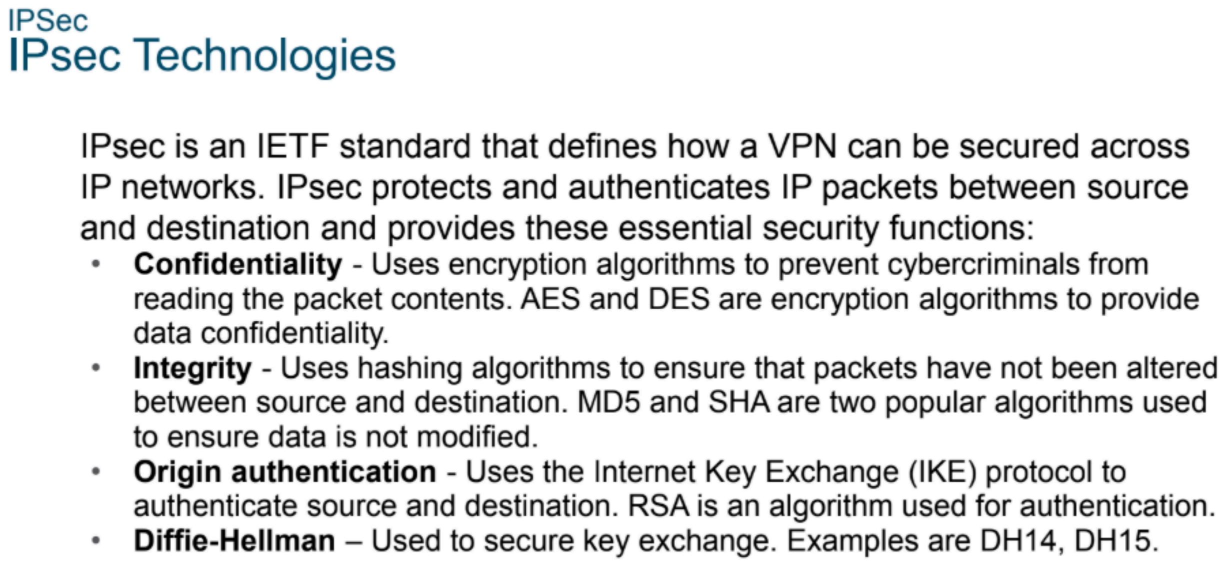
2. Enterprise managed VPNs can be deployed in two configurations. Explain TWO (2) types of Enterprise managed VPNs.

Q3

3. What is the difference between IPsec and SSL VPNs?

Q4

4. a) Illustrate IPsec framework which consists of essential security functions such as Confidentiality, Integrity, Origin authentication and Diffie-Hellman.



IPSec

IPsec Technologies

IPsec is an IETF standard that defines how a VPN can be secured across IP networks. IPsec protects and authenticates IP packets between source and destination and provides these essential security functions:

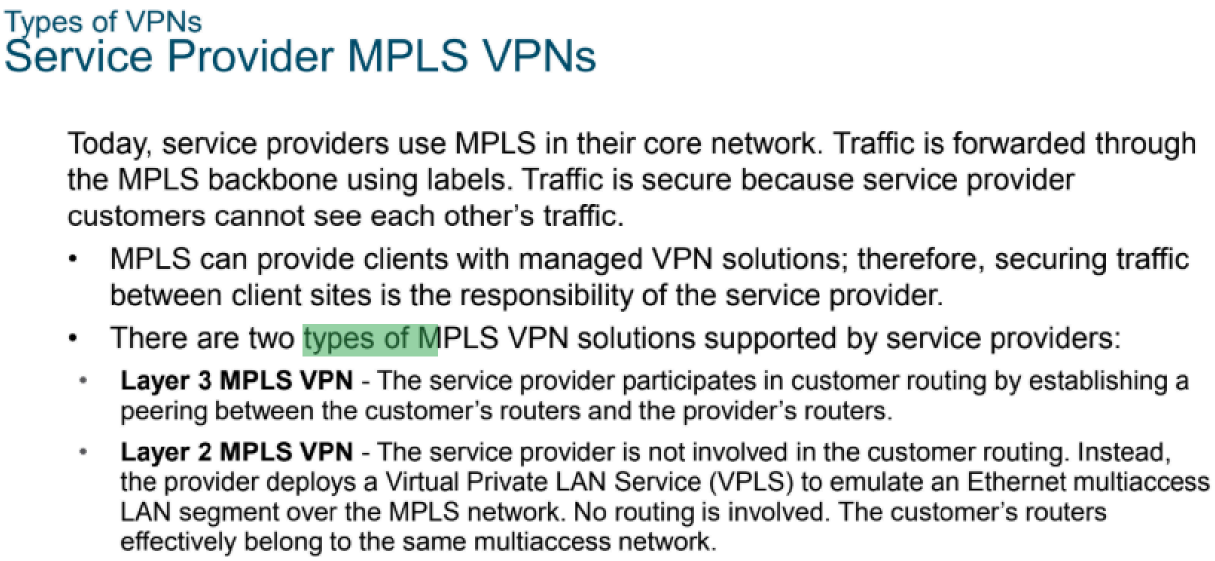
- **Confidentiality** - Uses encryption algorithms to prevent cybercriminals from reading the packet contents. AES and DES are encryption algorithms to provide data confidentiality.
- **Integrity** - Uses hashing algorithms to ensure that packets have not been altered between source and destination. MD5 and SHA are two popular algorithms used to ensure data is not modified.
- **Origin authentication** - Uses the Internet Key Exchange (IKE) protocol to authenticate source and destination. RSA is an algorithm used for authentication.
- **Diffie-Hellman** – Used to secure key exchange. Examples are DH14, DH15.

b) Explain two examples for each security function to protect data.

- *Confidentiality - For example, AES and DES are encryption algorithms to provide data confidentiality.*
- *Integrity- For example, MD5 and SHA are two popular algorithms used to ensure data is not modified.*
- *Origin authentication - For example, IKE and RSA algorithm*
- *Diffle-Hellman. For example, DH14 and DH15.*

Q5

5. Illustrate TWO (2) types of MPLS VPN solutions supported by service providers.



Types of VPNs

Service Provider MPLS VPNs

Today, service providers use MPLS in their core network. Traffic is forwarded through the MPLS backbone using labels. Traffic is secure because service provider customers cannot see each other's traffic.

- MPLS can provide clients with managed VPN solutions; therefore, securing traffic between client sites is the responsibility of the service provider.
- There are two types of MPLS VPN solutions supported by service providers:
  - **Layer 3 MPLS VPN** - The service provider participates in customer routing by establishing a peering between the customer's routers and the provider's routers.
  - **Layer 2 MPLS VPN** - The service provider is not involved in the customer routing. Instead, the provider deploys a Virtual Private LAN Service (VPLS) to emulate an Ethernet multiaccess LAN segment over the MPLS network. No routing is involved. The customer's routers effectively belong to the same multiaccess network.

Q6

6. What is the term used to describe the encapsulation of GRE over IPsec tunnel?

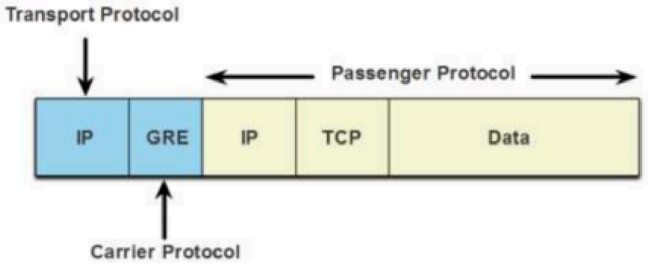
- *Passenger protocol, carrier protocol and transport protocol*
- *Passenger protocol - encapsulate original packet.*
- *carrier protocol - encapsulate original passenger packet*
- *Transport protocol - forward the packet*

Types of VPNs

GRE over IPsec (Cont.)

The terms used to describe the encapsulation of GRE over IPsec tunnel are passenger protocol, carrier protocol, and transport protocol.

- **Passenger protocol** – This is the original packet that is to be encapsulated by GRE. It could be an IPv4 or IPv6 packet, a routing update, and more.
- **Carrier protocol** – GRE is the carrier protocol that encapsulates the original passenger packet.
- **Transport protocol** – This is the protocol that will actually be used to forward the packet. This could be IPv4 or IPv6.



Transport Protocol

Passenger Protocol

IP

GRE

IP

TCP

Data

Carrier Protocol