SCII/00825/2019
MICHAEL ORINA
DATA COMMUNICATION AND NET TECH ASSIGNMENT ONE

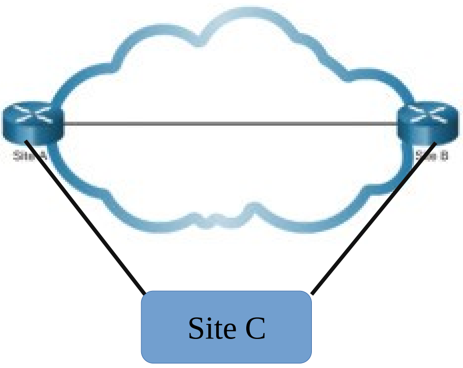
QUESTION ONE:

i. Identify at least two items at every site that needs upgrading [2 marks]

The network topology at every site
The 10 base 5 Ethernet cables at every site needs to be improved

ii. How many WAN connections will it take to connect the three sites? Show the links in a diagram [2 marks]

Three point to point WAN connections will take to connect the three sites



iii. What type of device could be used to connect the multiple signals from both voice and data and put them on the same WAN link? [2 marks]

A multiplexer (MUX) is a device that can receive multiple input signals and synthesize a single output signal in a recoverable manner for each input signal. It is also an integrated system that usually contains a certain number of data inputs and a single output

iv. What type of connectivity device should be used to connect the LAN to the multiple paths in the WAN created? What IP addresses should be used for the LANs/ WANs [2 marks]

Routers. A router is a hardware device that connects two or more networks. Routers are the primary backbone device of the Internet, connecting different network technologies into a seamless whole.

LANs uses private IP addresses

WANs uses public IP addresses

v. Discuss the media that is suitable for individual the branch offices, stating the merits and demerits of each media. [5 marks]

Coaxial cable. Electrical cable consisting of an inner conductor surrounded by a concentric conducting shield, with the two separated by a dielectric (insulating material) and a protective outer sheath or jacket

Merit
carry high-frequency electrical signals with low losses

Demerits

Signal leakage

Noise interference

Twisted pair. Type of wiring in which two conductors of a single circuit are twisted together for the purposes of improving electromagnetic compatibility.

Merits
reduces electromagnetic radiation from the pair and crosstalk between neighboring pairs and improves rejection of external electromagnetic interference

Demerits
It can be used up to cable segment lengths of about 100 meters only.

Fiber optic cable. It is an assembly similar to an electrical cable, but containing one or more optical fibers that are used to carry light providing a high-speed data connection

Merits
Bandwidth is higher than copper cables.

•Less power loss and allows data transmission for longer distances.

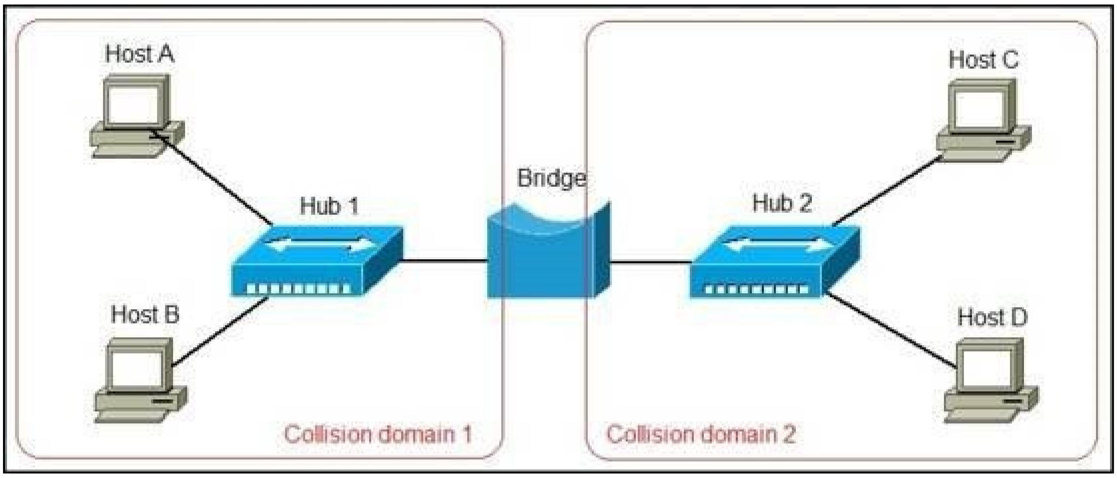
•The optical cable is resistance for electromagnetic interference.

Demerits
The optical fibers are difficult to splice, and there are loss of the light in the fiber due to scattering

QUESTION 2

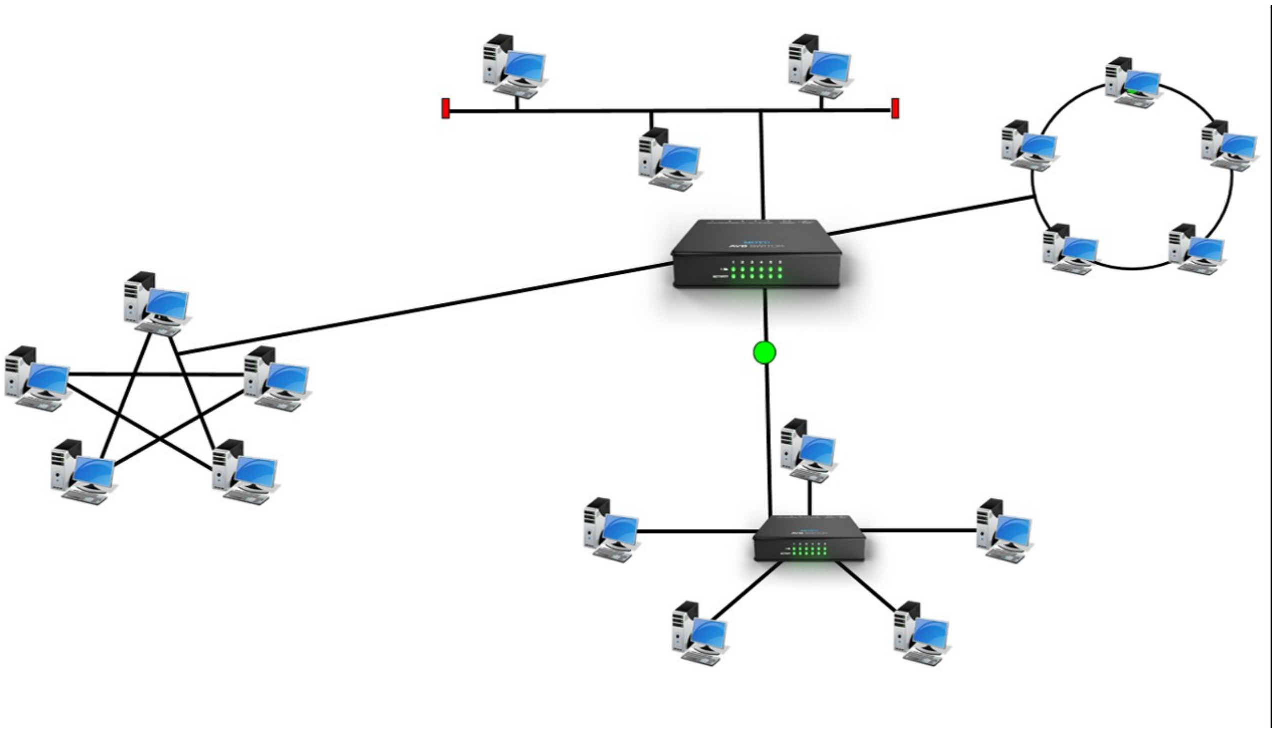
(a) **With the aid of a diagram describe how the following devices are implemented on a network, stating their roles. [10 marks]**

i. Bridge



A network device that connects multiple LANs (local area networks) together to form a larger LAN

ii. Router

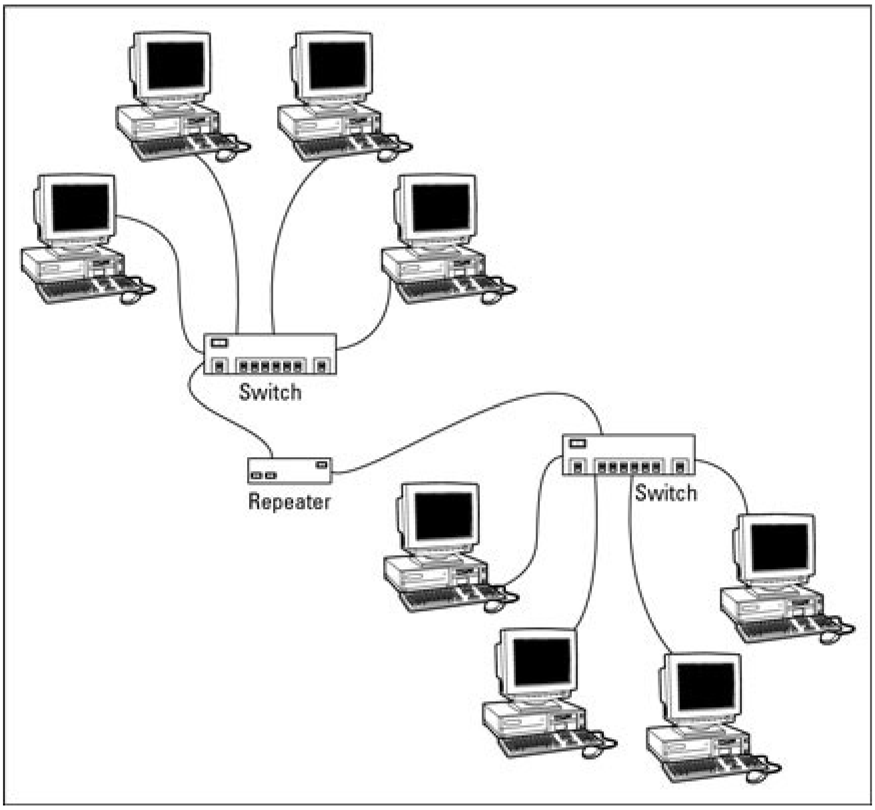


A router is a networking device that forwards data packets between computer networks

iii. Hub

A hub is a physical layer networking device which is used to connect multiple devices in a network

iv. **Repeater**



A repeater is an electronic device that receives a signal and retransmits it. It receives the signal before it becomes too weak or corrupted. It regenerates the bit and forwards the refreshed signal

(b) **Describe the implementations of Virtual Private Networks and how the various VPN security protocols secure Virtual Private Networks against attacks [10 marks]**

Site-to-Site VPN

Step 1 Configure Interesting Traffic

We need first to define the Interesting Traffic, that is, traffic that we want to encrypt. Using Access-Lists (Crypto ACL).

Step 3 Configure IPsec transform set (phase 2)

The goal of Phase 2 is to establish a secure IPSEc session between peers. We negotiation of IPSEc security parameters and IPSEc transform set. It represents an IPsec security protocol (AH or ESP) plus the associated algorithm. Multiple transform set can be configured. During the negotiation, the peers search for a transform set that has the same criteria. When found, it is applied to the protected traffic as part of the IPsec SAs of both peers. Therefore we create the transform- set VPN-SET to use esp-3des and esp-sha-hmac. To define a transform set

Step 4 Create a crypto ACL

In this step, we create the crypto map xx that combines the needed configuration parameters of IPsec Sas. Only one crypto map can be set to a single interface. If more than one crypto map entry is created for a given interface, use the sequence number.

Step 5 Create and apply the crypto map.

Apply the crypto map to the outgoing interface of the vpn tunnel. Then ensure that the routing information needed to send packets into the tunnel is configured.

Fig20. Applying the crypto maps.

Fig 21. Five steps of IPSEC configuration.

Fig 22. Site to site topology using packet tracer.

1.Remote Access VPN

1.Put a host name to router, Put an IP to the two interfaces.

2.Configure the Authentication for remote user.

There are a couple of different ways to authenticate and authorize remote users in order to access network resources via the VPN. The Authentication, Authorization, and Accounting mechanism (AA) of the router is used for such a task. The simplest way is to use Local usernames/passwords configured on the Router for authentication and authorization.

Remote users must be authenticated first to login to the VPN tunnel, and then must beauthorized to use the network resources. Therefore, we must configure the router device for both loginauthentication and network authorization.

3.Create username and password

4.Create pool of IPs to remote user

Configure an IP address pool that will be used to assign IP addresses to remote users

Remote access VPN.

5.Create apolicy between two routers

6.Create a policy and parameters that a specific group give to the client

7.Encrypt key to encrypt payload

These steps have similarities with site-to-site VPN configuration where we had one site with a dynamic IP address. Since the IP address of the remote VPN users will be unknown (dynamic) to the central site router, we have to create a dynamic crypto map.

8.Create a dynamic map for remote client profile

9.Create static map, define which client use dynamic map

10.Apply static map on specific interface