Q1)

As we can see in the give figures, we can see, two networks that have router, switch, web, email, database, and application server. At first, router is used to connect with the servers. Then, it is followed by firewalls to defend the system form cyber-attacks. Lastly, switch is used to communicate with the servers. The objective of this system is to fulfill client requests.

In figure 6-7, When a request is generated from the internet, it reaches to the router. The request obtained by the router is then checked by a firewall to avoid any malicious or harmful request. If the required information by the client is felt harmful or suspicious by the firewall, then it is filtered out. The request then reaches to Switch whose work is to deliver the request to the destination server. The required task is then carried out by the server and then sent the outcome back to the internet.

Figure 6-9 is slightly different than figure 6-7 as we can see a DMZ (Demilitarised Zone) between two server and two different firewalls connected to the switch. Web server and Email server is available for public whereas Database server and Application server is kept private and hidden. If a request is being trying to be made to a web server or Email server, it will first go through router followed by firewall that filters any malicious or harmful request then goes through switch and finally reaches to the destination server and returns the outcome. But If the request is made for the database server and application server, the request again goes through another firewall, which again filters the request then passes on to switch before reaching the destination server and again outcome is sent back to the internet.

The importance of design in figure 6-9 are:

* Two firewalls are there to protect the DMZ.
* Security and performance of the whole system is increased.
* Web and Email server are easily assessable whereas Database and Application server are highly protected.

Q2)

Network Address Translation (NAT) is a process in which various local private addresses are mapped to public address before the transfer of the data and information’s. Numerous devices are being used by a single IP address because of NAT.

Suppose your laptop is connected to your home router. Then someone found a way to the restaurant from their Laptop. This request is sent as a packet from the laptop to the router, which forwards it to the web. However, the outgoing IP address from a private local address to a public address should be first translated by the router. The receiving server does not know where to return the information if the package has a private address. This is like sending a physical email to find a reply service but using an anonymous reply address. Thanks to NAT, information is sent back to the laptop through the router's public address, not the private address of the laptop (Anon., n.d.).

It is used for many reasons such as:

* Reusing the private IP address.
* Better security
* Suitable IP spaces

Q3)

**SNMP version 3**

The SNMP version is one of the Simple Network Management Protocol whose management framework is more involved in terms of security.

The SNMP Version 3 has capacity to allows safe access to devices by authentication and encryption of data packets sent across the network.

**DNSSEC**

Digital signature is used to improvise the DNS authentication which uses public key cryptography. In this system, DNS data is signed by the person cryptographically**.** DNSSEC is a set of Internet Engineering Task Force extension standards for protecting data sent in the Domain Name System in Internet Protocol networks.

**SFTP**

The secure file transfer protocol is a process in which data is encrypted and transferred in a secured way.

SFTP sends files via a single channel, limiting the chance of hostile actors gaining access to sensitive information.

**SRTP**

SRTP is a security profile for Real-Time Transfer Protocol that adds message authentication, replay protection, and secrecy to the protocol. SRTP guarantees the secrecy of RTP and RTCP payloads, as well as the authenticity of all RTP and RTCP packets, as well as coverage over replayed packets.

**IPSEC**

IPsec (Internet Protocol Security) is a set of protocols that encrypts network traffic over IP networks. It secures IP network traffic by encoding confidential information, authenticating users, preventing replay attacks, and maintaining data confidentiality.

# References

Anon., n.d. *Comptia.* [Online]   
Available at: https://www.comptia.org/content/guides/what-is-network-address-translation  
[Accessed 08 06 2022].