Tracy Marie Andrea Madresta BSIT-3A February 26, 2023

**Network Administration**

**Network Topology**

According to GeeksforGeeks, network topology is the arrangement of a network that comprises nodes and connecting lines via sender and receiver.

There are two types of network topologies. The physical and logical topology. Physical topology is the interconnected structure of a network, this is the connecting of devices on the network with cables and wires. Logical Topology it refers to how and why the network is arranged the way it is and how data moves through it.

*Reference:*

<https://www.dnsstuff.com/what-is-network-topology#what-is-network-topology>

<https://www.geeksforgeeks.org/types-of-network-topology/>

**Router and Switch**

According to tutorialspoint.com, both router and switch are networking connecting devices.

Routers store data and deliver them in a form of packets. Switches are network devices that route data from multiple input ports to a certain output port. In others words, a router connects multiple networks, while switches connect multiple devices in a network.

*Reference:*

<https://www.tutorialspoint.com/difference-between-router-and-switch#:~:text=Routers%20store%20the%20data%20and,multiple%20devices%20in%20a%20network>.

**Firewall**

Firewall according to checkpoint.com, is a network security device. It monitors and filters incoming and outgoing network traffic. Its essentially the barrier that sits between a private internal network and the public internet.

A firewall is a part of any security architecture and takes the guesswork out of host level protections and entrusts them to your network security device.

We need firewalls to ensure the security of our devices because these can block malware and application-layer attacks to our devices.

*Reference:*

<https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/#:~:text=A%20Firewall%20is%20a%20network,network%20and%20the%20public%20Internet>.

**Virtual Private Network**

Virtual Private Network or VPN is a service which helps you stay private online. It establishes a safe and secure connection between your computer and the internet. It also provides a private tunnel for your data and communication while you use public networks.

We need VPN for the purpose of having privacy in the internet. It will act like an invisibility cloak that will hide everything you do on your phone or computer.

*Reference:*

<https://www.avast.com/c-what-is-a-vpn#:~:text=VPN%20stands%20for%20%22virtual%20private,while%20you%20use%20public%20networks>.

**Remote Access**

According to an article in hpe.com, a remote access is the ability of users to access a device or a network from any location. Through remote access users can manage their files that are stored in a remote device, this would allow them to have productivity anywhere.

Remote Access can be done through two different channels, the inter and local networks. Via the internet remote access use a virtual private network that will provide a secure communication between two devices. It will serve as a gateway at the edge of the network, sending it to the right hosts within the network. A local network on the other hand, makes a wire connection between endpoints using a private data channel rather than the internet.

*Reference:*

<https://www.hpe.com/us/en/what-is/remote-access.html#:~:text=Remote%20access%20is%20the%20ability,collaboration%20and%20productivity%20from%20anywhere>.

**Network performance optimization**

According to obkio.com, Network optimization refers to the techniques, best practices and tools used to monitor and improve a network performance. This could include network troubleshooting and upgrading a network etc.

Network Optimization all about identifying network problems, improving network performance with concrete changes, and comparing performance before and after making changes.

*Reference:*

<https://obkio.com/blog/network-optimization-how-to-optimize-network-performance/#:~:text=In%20short%2C%20Network%20Optimization%20refers,%2C%20upgrading%20your%20network%2C%20etc>.

**Network Monitoring and Logging**

Network Monitoring is the process of constantly monitoring a computer network for problems such as slow traffic or component failure, according to vmware.com.

To maintain network integrity, it is critical to perform continuous network monitoring. Network monitoring also has benefits, such as visualizing the flow of data across devices and networks this enables network administrators to quickly identify and remediate any problems that will occur.

*Reference:*

<https://www.vmware.com/topics/glossary/content/network-monitoring.html#:~:text=Network%20monitoring%20is%20the%20process,slow%20traffic%20or%20component%20failure>.

Network Logging is a process of keeping information and all interactions made in the system or application, according to study.com. It needs network maintenance to ensure effectiveness of tools that is used over time.

It serves as a recording of all activity that a system conducts in its operations. It’s a file that contains a record of events that occurred in the application. It contains the user records and process access calls to objects, attempts at authentication and other activity.

*References:*

<https://study.com/academy/lesson/network-logging-definition-tools.html#:~:text=Network%20logging%20is%20a%20process,network%20logs%20and%20synthesize%20logs>.