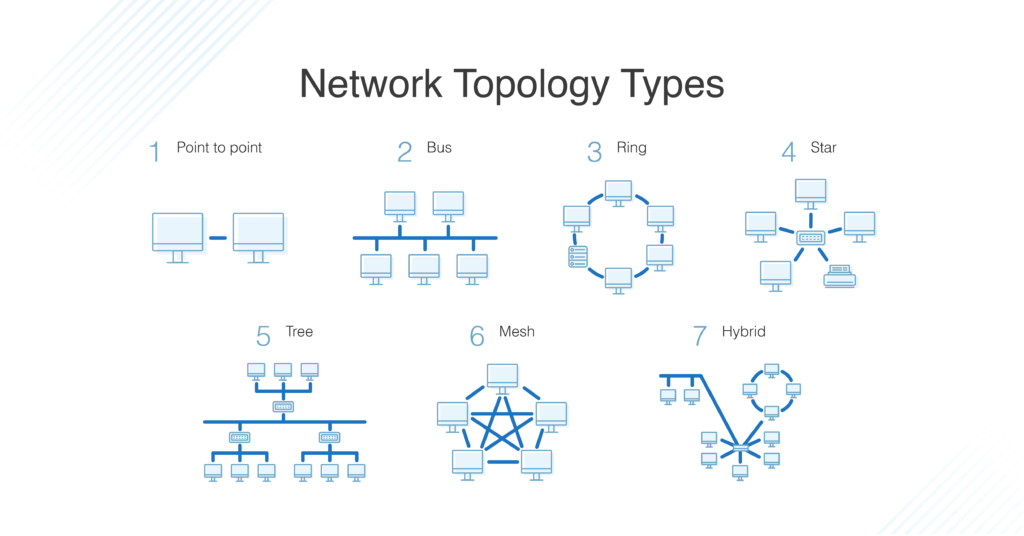
**Tiano, Kiana Crizel R. BSIT 3A**

*System Administration and Maintenance*

* **Network Topology** is the arrangement of nodes such as the switches, routers, etc., and connections in a computing network. This incorporates the logical and physical links of how network devices relate to each other.

Network Topology has different types, most known includes:

1. Point to Point Topology – it directly connects two devices in a network.
2. Bus Topology – also known as “line topology” as all devices are arranged and connected on a single cable following a single direction. Data also flows in a single direction.
3. Ring Topology – each device has exactly 2 neighbors as they are arranged on a circle/ring allowing data to travel in both directions, thus limiting that data can only travel in one direction at a time as ring topology is half-duplex.
4. Star Topology – all networking devices are directly connected in a single central hub/server.
5. Tree – networking devices are connected through parent-child hierarchy extending like a branch of networks.
6. Mesh – all devices are interconnected with each other like a web.
7. Hybrid -this setup is a combination of 2 or more network topologies, such as it integrates multiple network structure.



* **Router and Switch**

A switch is used to connect all networking devices such as the printers, computers, and servers for a small network. It allows connected devices to exchange and pass information and share data directly.

In setting up for big business network, a router is used. A *router* is used for connecting multiple switches and networks. It facilitates the routing of information, directing traffics, and managing ports and VLAN security settings.

* **Firewall** functions to monitor, allow, and block network traffics based on a given security protocols. It is a first line of defense network security device that distinguishes secured and controlled internal networks from suspicious external networks including the internet.
* **VPN** orVirtual Private Network protects a device from cyber threats and attacks when using a public network connection. It secures the network connection by encrypting the device’s internet traffic, as well as disguising online identity making it less susceptible to such cyber-attacks.
* **Remote Access** allows users toperform operations and accesson a device regardless of their location and distance. This means that users can access their files, shutdown, etc. anytime and anywhere using the remote access.
* **Network Performance Optimization**

Network performance optimization boosts the overall network experience through security, reliability, and speed enhancement for enterprise networks.

To monitor, manage, and improve network performance and functionality, a variety of technologies, tactics, and best practices are utilized. The main purpose of network optimization is to give all users a quick and effective network experience. Monitoring and improving network performance is a continual process that is always being modified to satisfy changing demands for performance.

Some examples of network optimization tools and techniques include:

* The use of traffic control mechanisms and technologies by Quality-of-Service (QoS).
* Leveraging an SD-WAN (software-defined wide area network)
* Data Compression
* **Network Monitoring and Logging**

Network Monitoring Log records every event of transaction that occurs on a server, computer, or other piece of network hardware. It is also known as the “journal-of-record”.

Examples include:

* Windows Event Log files produce by Microsoft
* System Log (also known as Syslog) used by UNIX-based servers and devices
* W3C/IIS log files by IIS and Apache

To lessen an organization's vulnerability to hackers, viruses, damage, loss, and legal obligations, log files provide plenty of information. To comply with regulatory compliance criteria and to compile reports, log data must be gathered, kept, analyzed, and monitored.