**Network Administration**

Franz Dave E. Apid BSIT3A

CIT 218 System Administration and Maintenance

**1. Network Topology** - A network topology is the physical and logical arrangement of nodes and links in a network. Nodes typically include devices such as switches, routers, and software with switch and router capabilities. Network topologies are frequently depicted as graphs.

Network topologies describe how networks are organized and where traffic flows are located. Administrators can use network topology diagrams to determine the best locations for each node and the best path for traffic flow. A well-defined and planned-out network architecture allows an organization to more easily discover problems and resolve difficulties, enhancing data transfer efficiency.

Network topology has a significant impact on how a network operates. The topology, in particular, has a direct impact on network functionality. Selecting the right topology can assist boost performance since a well-chosen and maintained network topology improves energy efficiency and data transmission rates.

**2. Router and Switch** - Switches and routers are the two most important pieces of equipment to have when setting up a small office network. Despite their similar appearance, the two devices provide distinct tasks within a network. Switches allow resource sharing by linking all of the devices in a small company network, including PCs, printers, and servers. Because of the switch, these connected devices can share information and communicate with one another regardless of where they are in the building or on campus. A small business network cannot be built without switches to connect devices.

Similar to how a switch links various devices to form a network, a router links various switches and the networks they each create to create a much larger network. These networks could exist in a single location or in several locations. One or more routers are required when setting up a small business network. The router links various networks together while also enabling networked users and devices to access the Internet.

**3. Firewall** - A firewall is a network security device that monitors and filters incoming and outgoing network traffic depending on previously set security policies in an organization. A firewall, at its most basic, is a barrier that lies between a private internal network and the public Internet. The primary function of a firewall is to allow non-threatening traffic in while keeping harmful traffic out.

**4. VPN** - VPN is an abbreviation for "Virtual Private Network," and it refers to the ability to establish a secure network connection while utilizing public networks. VPNs encrypt your internet traffic and mask your identity online. Other parties will find it more difficult to trace your online activity and steal data as a result. Encryption occurs in real time.

VPN conceals your IP address by routing it through a specially configured remote server managed by a VPN host. This implies that if you use a VPN to access the web, the VPN server becomes the source of your data. This means that your ISP and other third parties cannot know which websites you visit or what data you transmit and receive online. A VPN acts as a filter, converting all of your data into gibberish. Even if someone were to obtain your data, it would be worthless.

**5. Remote Access** - Remote access refers to the capacity to connect to a system or network, whether it's a personal device or an office server, without physically being present. Employees can operate off-site, such as from home or elsewhere, while yet keeping secure access to a remote computer or network. Remote connection adds versatility. Remote access may assist off-site workers feel linked to a firm's ecosystem, whether a small business wants to enable volunteers to work from home or a major corporation needs to connect software developers working from off-site locations.

**6. Network Performance Optimization** - Network optimization refers to the tools, strategies, and best practices used to monitor and optimize network performance. These network optimization approaches may involve network monitoring, network troubleshooting, network upgrades, and so on.

Network optimization is all about:

* Identifying network problems/ areas for improvement
* Improving your network performance with concrete changes
* Comparing performance before and after making changes

Optimizing your network is the key to help improve network performance. It helps provide optimal performance of your Internet, VPN, Firewall, VoIP and UC apps, and most importantly user experience.

**7. Network Monitoring and Logging** - Every event or transaction that takes place on a server, computer, or piece of network gear is documented in a Network Monitoring log. There are logs almost everywhere in your IT infrastructure. Microsoft systems produce Windows Event Log files. UNIX-based servers and devices adhere to the System Log (or Syslog) standard. Apache and IIS create the W3C/IIS log files.