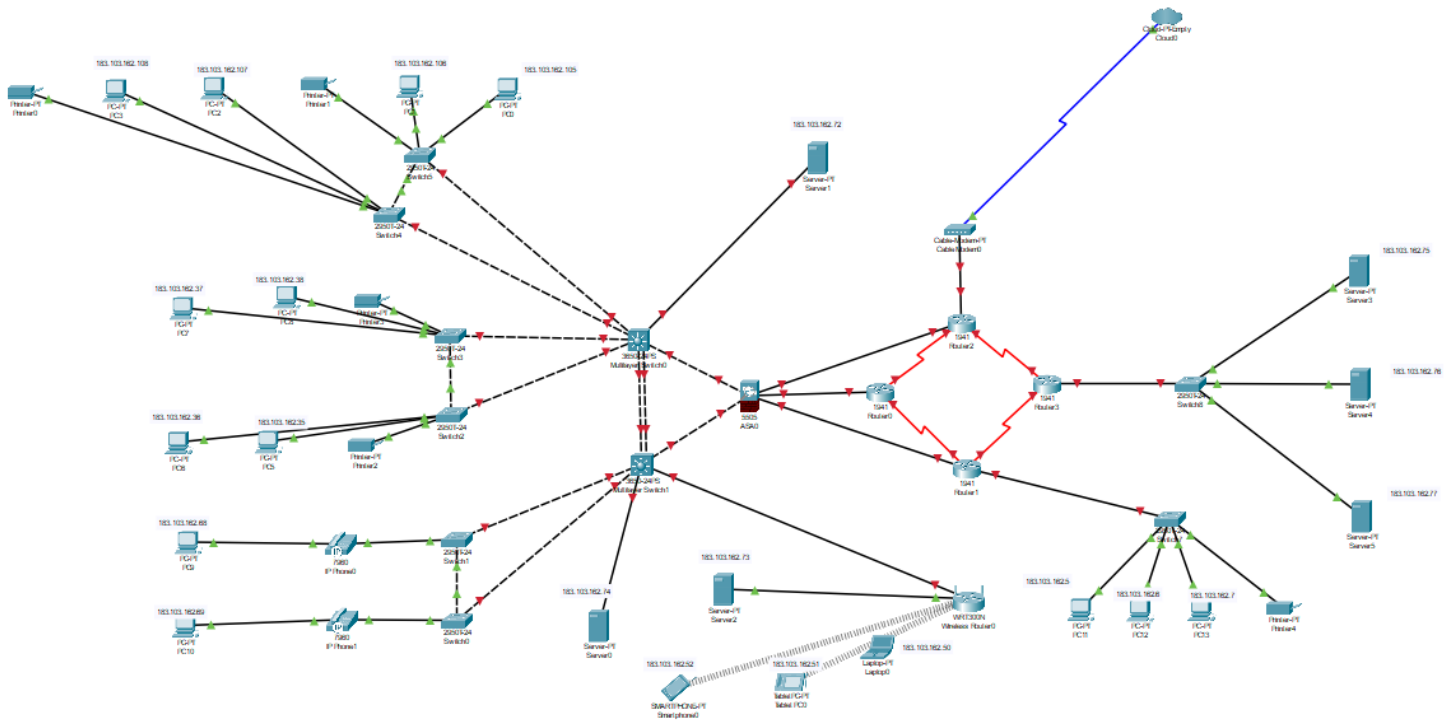
Enterprise Network Design



A computer network refers to a collection of computers and other electronic devices such as printers linked together using physical wires or wireless means. The connection is used to facilitate the flow of data between them. A computer network enables particular users to enter data using one computer to be store the information in central storage and be shared with other users on the same network. Various components are used to develop computer networks. These components include topologies, cabling systems, internetwork devices such as routers and switches, security devices such as firewalls and anti-intrusion prevention detections, key servers such as DBMS and WIFI capabilities. This paper will discuss why I used the listed components to design a office environment network, how they function, how the network design will be secure by using these components, and any type of redundancy that will be necessary for security reasons.

Network topology is one of the most essential components used by network specialists to design a network. Network topologies refer to the physical and logical arrangement of various nodes and devices in a network. Physical topologies determine the physical connection and layout of the nodes in a network while logical topologies determine how data packets in a signal travel from one device to the next on a network. The layout of a network topology is significant in determining the performance of the network. The design of a network

topology determines the easiness of locating faults, troubleshooting errors, and making the efficient allocation of resources. In my opinion, the star topology would be the most efficient form of physical topology to design a network. The star topology would enable the network administrator to manage a network from a single location. Besides the central hub, the failure of a single node would not affect the performance of the other nodes. Consequently, a single node could be added, removed, or modified without requiring the entire network to go offline. Therefore, a star topology would be preferential to expand the network (Barranco, Proenza, & Almeida 811). Besides, the cost of establishing the network would be fairly cheap because of requiring little cabling when compared to other physical topologies.

Cabling is another essential component to designing a network. During the process of cabling, I used the structured cabling system. Structured cabling refers to an infrastructure formed by smaller and standardized elements in a building or across a campus. Structured cabling supports transmission of data, video, multiple voices, and several management systems such as security access (Balubal, et al. 351). Structured cabling also increases the ability of the network to support rapidly - advancing technology in the workplace. In the past, networks used point-to-point cabling where each hardware component had its cable. As the network expanded, point-to-point cabling would result in a jumbled mess of cables and wires that could be unplugged accidentally and present safety hazards such as tripping. Besides, point-to-point cabling made it difficult for a component to be added, removed, or changed in a network. Therefore, structured cabling improves the organization of the cables making it easy for network specialists to conduct maintenances and help businesses to improve the return of investments. Structured cabling has six subsystems which include entrance facilities, equipment rooms, backbone cabling, horizontal cabling, telecommunications room, and work area components. Structured cabling is better than point to point cabling because of being cost-effective, time - saving, and mitigating the risk of downtime. Cat 5 and 6 unshielded twisted pair cables and fiber optics are the best cables to use because of their large bandwidth and high speed.

Network and internetwork devices are also essential components used by me to design that network. Internetworking devices refer to hardware within networks that are used to link different nodes in a network. Some of the key internetwork devices include routers, switches, hubs, modem, repeaters, and access points.

Routers are used in a large network to chart the best pathways in a sea of interconnected devices to facilitate the transfer of data packets from the source to the destination (Lockwood, et al. 160). Routers function as intelligent devices which store information concerning the networks that they are connected making it possible for me to determine the best pathways. Hubs are used in a computer network to connect multiple devices. Besides, they function as repeaters by strengthening and amplifying weak signals that have attenuated after traveling long distances through the cables. Switches are used to improve the efficiency of networks by performing the functions of routers and hubs. Switches can also read the addresses of hardware components in a network and transmit incoming data packets to the appropriate destination. Modems are used to convert digital signals into analog signals for them to travel over analog medium and revert the analog signals into digital signals in the receiving end. Repeaters are used to amplify weak signals and retransmit them over long distances. Access points are commonly used to connect wireless devices into a network.

Network security plays a significant role in protecting workstations from harmful spyware and interception during transmission. There are various security devices used by me to develop strong network security. These security devices include firewalls, intrusion detection systems, unified threat management, network access controls, and anti-virus. Firewalls are used to exclude undesirable and unwanted network traffic from gaining access to network systems of an organization. Firewalls allow or prevent access to a network through whitelisting, that is denying all connections except those listed as acceptable, or blacklisting, that is allowing all connections except those listed as unacceptable. Intrusion detection systems are used to enhance cybersecurity by spotting malicious software and hackers on a network to enable their prompt removal from the network and prevent data breaches as well as using data logged about the event to create a better defense against such attacks in the future (Shu, et al. 770). Computer networks can also use unified threat management systems to install software or hardware that conducts multiple security functions such as content filtering, antivirus, and intrusion prevention. Unified management systems are more preferable than multiple products because of enabling single management of security. Network access control is used to restrict the availability of network resources to remote devices that comply with a specified security policy such as a requirement of having the safest antivirus.

Servers are also important components in the design of a computer network. Servers are used to provide programs, services, data, and resources to other computers known as clients. In peer to peer networks, computers can function as servers and clients at the same time (Qureshi 197). Servers are usually configured to listen to the request and provide servers to clients on the network. There are several types of servers that provide different services to client computers. For instance, file servers are used to store and distribute files belonging to client computers. The hardware of the file servers can be designed to maximize the speeds of reading and writing to improve their performance. Print servers are used to perform printing requests for several clients in the network. Web servers are the most common types of servers that host data and programs requested by users across an intranet or internet. Database servers are used to perform database operations and respond to requests concerning retrievals of certain files by the clients. Servers have more advanced hardware and storage compared to client computers. Several operating systems are used to run servers. These operating systems include Microsoft Windows servers, Linux/Unix servers, and NetWare and cloud servers. These operating systems help servers to listen and respond to the request of client computers.

As a network designer in this project I must build a reliable network. Any type of computer network breakdowns such as equipment failure, human error, and cyber-attacks can cause devastating consequences for the business. Backup systems need to be established to prevent one point of failure from disrupting the entire network. Redundancy is one of the main strategies that can be used to minimize the chances of failure of a computer network. In network redundancy, alternate instances of network equipment, devices, and communication mediums are installed within the network infrastructure to ensure network availability in the case of path failure or unavailability (Radetzki, et al. 6). When a network outage occurs, network redundancy helps network operators to swap network operations in the redundant infrastructure and ensure that the network continues to work normally. Some of the networking components incorporated in the redundancy designs include routers and switches, network protocols, subnetting connections, cloud recovery storage for data on the hard disks, processors, and power supply.

In conclusion, there are various components that I used to design that network. These components include network topologies, cabling, internetwork devices, network security systems, servers, and network redundancy.

The design of a network topology is significant because of determining the easiness of locating faults, troubleshooting errors, and allocating resources efficiently. The star topology is the best physical topology because of centralized control, easy adjustment, and expansion of the network. Structured cabling is essential in a network for improving the organization of cables and preventing accidents and safety hazards. Internetwork devices such as routers, switches, and modems are also important components for designing a network because of their significant role in connecting network nodes. Network security can be reinforced through the use of firewalls, intrusion detection systems, unified threat management, network access controls, and anti-virus. Servers are also essential components of a computer network because they listen and respond to the requests of the client computers. Network redundancy is also an important consideration when designing a network because of preventing breaking down of the whole network due to a fault of a single component or cyber-attacks.

Work Cited

Barranco, Manuel, Julián Proenza, and Luís Almeida. "Quantitative comparison of the error-containment capabilities of a bus and a star topology in CAN networks." *IEEE Transactions on Industrial Electronics* 58.3 (2009): 802-813.

Balubal, Charmaine B., et al. "Cabling and cost optimization system for IP based networks through Genetic Algorithm." *2014 IEEE REGION 10 SYMPOSIUM*. IEEE, 2014.

Lockwood, John W., et al. "NetFPGA--an open platform for gigabit-rate network switching and routing." *2007 IEEE International Conference on Microelectronic Systems Education (MSE'07)*. IEEE, 2007.

Qureshi, Anique A. *The International Handbook of Computer Networks*. Barming, Kent: Trentop Management Books, 2004. Print.

Radetzki, Martin, et al. "Methods for fault tolerance in networks-on-chip." *ACM Computing Surveys (CSUR)* 46.1 (2013): 1-38.

Shu, Zhaogang, et al. "Security in software-defined networking: Threats and countermeasures." *Mobile Networks and Applications* 21.5 (2016): 764-776.