Mitchell Fitzsimmons

6/18/2023

IT 212

Final Project

Understanding the OSI stack relationship to modern communication networks helped the design, and aids in understanding some of the choices that have been made. The OSI stack layers are as followed: application, presentation, session, transport, network, data link, and physical layers. These layers are seen as protection or access points for different entities. Knowing that companies want security and functionality in their networks, and understanding the OSI stack layers helps keep these ideals in the forefront of network design.

Important things to consider or have would be email facilities for corporate, video conferencing capabilities, basic internet access, and data protection and encryption through firewalls and such. There are three modes of data transport that should be supported on this network. First, is the half duplex, where data is unidirectional and goes one way. Next, there is half-duplex, which can have information travel both ways, but only one at a time. Finally, there is the full duplex which allows information to go both ways at the same time. Also, the network set up here will have some hardware requirements that would include a hub, gateway, switch, router, bridge, modem, and more. IP range is also important for a new network like this. I would use IP range class c, 192.168.1.1. This would give them over 60,000 host addresses (192.168.0.0 - 192.168.255.255).

In regard to LAN topologies there are many that could be sued. First a mesh topology could be used which would allow every system to be connected to every system. Next, we could use star topology and have everything connect using point to point connection. Finally, and also the best topology for the project is hybrid. This allows a combination of the different methods. This is best because it allows them to connect systems how they want to be connected, while also being easy to accommodate any future growth.

There are a few things to consider when setting up this network. Keeping the current size of the company, projected and desired growth, and understanding what actions will be performed on this network will help initial instillation. Given the scenario and prior research, I believe Spectrum is the best choice for the company compared to cable internet. Cable can have issues with bandwidth (general traffic congestion), and can have outages at peak usage times, and is simply not as fast as fiber-optic. Spectrum has high speed internet up to 1 Gbps, which is more than ideal for the office. They should be able to perform different tasks simultaneously without any worries due to bandwidth. They also claim a 99.9% reliability in terms of there network. For these reasons I believe spectrum is the ideal choice.

In terms of the software and hardware needed by the company for the network and their general daily activities, there is a list. The office will have an internal server that the network administrator will have set up Windows Server 2022 with active directory. This will help contain whom has access to what on the network making it more secure. Zoom is a great online meeting tool that has been used very often over the last few years and is reliable. Using VoIP and Zoom, the company should be able to communicate within and outside the office, while maintaining a level bandwidth. Next is the print configuration. There should be about 4-5 printers in the building, all able to print locally from the company, as well as, through a file share server so that remote workers can still print the necessary documents they need to. One of the printers in the group should be kept for executive and manager use, limiting those who can print from it. Finally, for the last of the software, all computers within the company should have anti-virus and security procedures, as well as Microsoft Office and other general application that are used in daily activities.

As most things, in initial implementation and set up there may be unforeseen errors, and even foreseen errors. One of today’s biggest issues for companies that are network reliant are cyber attacks and information leaks. These can be detrimental to the reputation of a company, and can cost them large quantities of money. Knowing this there a few things that can be done preemptively to minimize damage. Firstly, proper security understanding and training for all staff members who regularly use the network. Using a few concepts like least privilege can help keep unwanted viewers and network users from having access to certain items. Basic training like impressing the importance of personal passwords (or even multi-factor authentication) can also help eliminate potential damage. Finally, having network monitoring software can help identify potential risks so action can be taken before damage occurs, or even just minimize damages. Software like Datadog, Dynatrace, and Entuity, are considered some of the best programs for this.