Ronald W. Sudol III

SNHU IT212

Final Project

12/10/2023

**Fayetteville, NC Network Design Recommendations**

This document shall layout key considerations and topology recommendations for a new office in Fayetteville, NC. The office will be the base of operations for approximately 50 employees that work both on site and from home. The network will also need to support teleconferencing and remote network and device management by the company’s IT team. The has access to fiber, cable, and T1 internet which are all decent choices for digital communications media. Given the distance between office locations, fiber will likely be the wisest choice as it is fast and efficient and maintains signal strength over longer distances. Given that remote access and video teleconferencing is essential, the mode of data transport will need to be full duplex, which will allow data to be transmitted and received simultaneously. This network will require common hardware like network switches, an internet router, and a network firewall. A subnet mask of 255.255.255.192 will allow for just over 60 usable IP addresses, which is ideal for the 50 employees accounted for at this location. For scalability, however, a subnet mask of 255.255.255.128 would allow for twice as many usable IP addresses, which may be desirable if we plan on the office growing in the near future.

Given the varied work styles of employees and the necessity of both security and accessibility, I would recommend a hybrid LAN topology known as a “star-bus” or “tree” topology. Devices can be grouped by physical office location (such as first floor, second floor, etc. …) or by role (sales, billing, marketing, etc. …). Each group of devices would be connected to a switch. Each of those switches would be connected to each other, either serially or as a mesh, as well as connected to the network firewall. The network firewall would then be connected to the internet gateway router. Employees working from home would simply need their work devices whitelisted on the firewall and they could access data from home.

Star topologies have a variety of strengths. Primarily they are easy to configure, add/remove devices to/from and are simple to troubleshoot. A weakness of a star topology is that it creates a central point of failure and if there is an issue with the single switch, all devices can lose connectivity. A full mesh topology can create a lot of unnecessary redundancies. By combining these approaches, we can create a hybrid network that is reliable, modular, and maintainable. This also allows for optimal support because IT personnel can remotely configure and maintain hardware on the network while still granting work-from-home employees the accessibility to retrieve work-related data from their workstations at home. This topology is also scalable so it can be added to without much disruption to the current network.

When considering an internet service provider, there are certain key considerations for identifying the optimal choice. Namely, we must consider speed, security, and reliability. For the Fayetteville, NC area, there are two optimum choices: CenturyLink and Spectrum. Spectrum advertises 1Gbps download speed and 35Mbps upload while Century link offers a balanced 940Mbps upload and download. Spectrum offers free antivirus and firewall protection while CenturyLink offers a broad array of advanced security features. In terms of reliability, both companies boast a rating that is just over 99%. Based on this analysis, CenturyLink would be the most appropriate internet provider for this location to meet the business’ goals and objectives. We will have our own firewall and anti-virus protections in place, so we won’t need what Spectrum offers. However, CenturyLink’s more robust security features will help to augment our own. Furthermore, CenturyLink offers comparable download speeds but significantly better upload speeds that will help to support our need for video conferencing and remote access.

When considering hardware and software solutions, we need to consider the operating system for our server, for our on-site workstations, plus the hardware and software for our printing, telecoms, faxing, and video conferencing needs. The servers will run on Linux as it is opensource and reliable. The best choice would likely be Ubuntu or Debian. The servers should also be set up with network management software to monitor and optimize network performance. The workstations should be set up with Windows 10 or higher. Telecoms would best be handled as a VoIP service implementing Yealink or Polycom desk phones managed with either 3cx or Netsapiens as these options are versatile and scalable. For video conferencing, the workstations should also be set up with webcams and noise cancelling headsets to reduce cross chatter, as well as conferencing software such as Teams. Printers should be fax capable and have associated Grandstream ATA devices to allow for faxing over the internet. Further, the printers should be managed with software that supports tracking, automated driver distribution and access control. Tracking allows users to see the status and history of their print jobs. Automated driver distribution ensures that users do not need to install any additional drivers or software on their devices. Access control allows users to share printers with other users based on predetermined permissions for each printer. The bandwidth provided by CenturyLink should also be more than adequate to meet our teleconferencing needs because “video conferencing typically requires around 1.5 to 2 Mbps down and 2 Mbps up for participants in a one-to-one call with two parties”(AIT, 2023). Even larger conference calls will not be slowed down with download/upload speeds at a rate of 940Mbps both ways.

There are a number of potential errors that can wreak havoc on any network. One of the most damaging issues is connectivity errors. Connectivity errors mean that network devices or users may experience intermittent or no connection to the internet or other network resources, due to faulty cables, misconfigured settings, or network congestion. In terms of internet outages, there is little on-network troubleshooting that can be done to address the error because the error is actually past the demarcation point. However, a failover connection to a second ISP can be established at the main router so if one service provider experiences an outage, the system can still connect to the internet via the second ISP connection. The chances of two ISPs having outages at the same time is significantly smaller and this method can help to avoid the network being cutoff from the internet entirely. For on-network connectivity issues, having dedicated switches for each type of sub-network creates a redundancy that isolates the issue to just the sub-network switch and its associated devices. This makes troubleshooting easier because the problem is already isolated which allows IT professionals to narrow the scope of their efforts to just the switch and associated devices presenting issues. Furthermore, trace routing can be executed to trace the path of packets and measure for latency, packet loss, and internal outages. Pinging network switches from the main router will help IT personnel discover if the switch is in fact connected to the network at all. Pinging devices from the affected switch will then help narrow down if the device governed by that switch are connecting to the network. A combination of the approaches and network design elements would ensure the resolution of the errors by anticipating and mitigating issues before they arise, providing useful information and feedback about the network status and performance, and by narrowing down the possible causes and solutions of the errors.

Maintaining a network requires that IT personnel be able to not just address issues when they arise, but also ensure that things are continuing to operate as intended via the practices of network monitoring, patch management, and inventory control. Network monitoring is the process of observing and analyzing the performance and availability of devices and services on the network. There are many open-source software options for network monitoring tools that can help to implement aspects of network maintenance, such as port scanning, interface monitoring, and packet flow monitoring. Patch management is the process of acquiring, testing, and installing updates or patches for your network devices and applications. This can best be achieved by setting up a separate test network that mimics the behaviors and configurations of the actual network and testing the patches by first installing them in the test environment to detect any potential conflicts with the current network state beforehand. Inventory control is the process of managing your network assets and resources. It involves discovering, tracking, and documenting your network devices and their configurations, locations, and lifecycles. There are numerous open-source software options available for inventory control that can streamline this task in addition to providing comprehensive data about individual devices on the network.

A diagram of a network

Description automatically generated

**Citations:**

Lammle, T. (2018). CompTIA Network+ Study Guide: Exam n10-007. John Wiley & Sons, Incorporated.

Small business internet service | CenturyLink. (2023) https://www.centurylink.com/small-business/business-internet/

Spectrum Business Internet | Spectrum. (2023) https://www.spectrum.com/business/internet

Advanced Internet Technology | Empowering Your Digital Future with Cutting-Edge Internet Solutions. (2023). https://www.ait.com/