SNHUEnergy Inc: Network Analysis and Architecture Evaluation

Jeremy Willett

**Executive Summary**:

This report to is assess the current company network architecture and provide recommendations on fixing and implementing changes to the network to streamline performance and allow scalability as the company proceeds with its planned expansion. The company currently uses most of its bandwidth on VoIP services and company applications. The current network is inhibited by the physical WAN setup as the entire Memphis office needs to run to the Dallas office to reach the internet. This report explains the reasoning behind implementing more routers, switches, and firewalls to provide better performance and security on the network. Additionally, the implementation of multi factor authentication devices, switching to virtual machines and adding a network monitor to the company network will aid in securing the company network, its’ data and aid in preventing issues from arising impacting business and clientele.

**Current Network Architecture**:

SNHUEnergy Inc., is a company with a network currently implemented into two different locations. The company’s different departments are separated between the two sites located in Dallas and Memphis. The Dallas office houses the payroll department, the accounting department, the HR department. The Dallas office houses the servers for each of these departments as well the internal E-mail server. The Memphis office houses the billing department and the operations department and the associated servers for these departments. The Dallas office acts as the hub for the company wide area network (WAN). The Memphis office workstations and servers are connected to a router via ethernet switch and in turn, connected to the Dallas location. The Dallas location connects the workstations and servers via switch to the Dallas router. The Dallas router connects the company WAN to the internet protected by a firewall. The network operates using TCP/IP protocol. This can be broken down and associated with the corresponding OSI model layers as shown in Figure 1. Diagram

Description automatically generated

Figure - Network diagram with labeled devices and corresponding OSI Layers.

Each component on the network serves a purpose. Each of these components use the different layers of the OSI model to display, transmit and receive data. The workstations are there to allow employees access to the network and the information contained within. They also serve as the main way to utilize the internet. The servers for each department and the E-mail all store the data for each of these services. Billing information is stored on the billing server, payroll information is stored on the payroll server, the same goes for E-mail, accounting, HR, and operations respectively. The switches act as a hub for all these devices to connect together. This is done because generally, a router does not have the number of ports on it needed for an office setting, as opposed to a home use router that would be ok with have only a few ethernet connection ports. The switches act as the hubs for all the hardwired devices to connect to that then allows a single connection out of the switch to the router. The router is responsible for connecting the local office network (which encompasses all the devices connected to the switches and any wireless access points) to the internet and to the Memphis location since it is located a greater distance away and would not function on the local network. The last component is the firewall. This serves to protect the entire company network from unauthorized outside access. The firewall servers as the virtual barrier between the network and those who should not be allowed access to it. If a router is the door to the networks house, then the firewall would be the fence around the yard of the property.

The entire network is designed to allow employees access to the internet and to information contained on the servers to facilitate day-to-day operations. The main interface for employees is their associated workstations. In each office, these workstations are connected to the servers on the site via ethernet switch. A physical ethernet cable from each workstation connects to a switch. The servers are also connected by ethernet cable to a switch. This switch is responsible for determining where a workstations connection needs to be connected and when. As an example, if a workstation in the Dallas office wants to access the E-mail server, there is no reason for the switch to direct the workstation connection to the router because the email server is located at the Dallas site, so the switch just routes the connection to the port on the switch that the email server is connected to. This routing would work differently for a workstation in the Memphis office. When attempting to access the same E-mail server from the Memphis site, the workstation is connected in the same manner to a switch. This switch connects all the devices at the site to the Memphis site router. The router then directs the connection to the Dallas router and through the Dallas router, to the necessary switch and finally reaches the E-mail server at the Dallas site.

With the way the network is currently set up, workstations at the Memphis site are at a major disadvantage when it comes to accessing the internet. The reason for this is because to access the internet, the communications over the network must travel to the Dallas location first, and then pass through the firewall and out to the internet. This results in an unnecessary amount of delay added to the connection as opposed to having a firewall and internet connection at the Memphis location as well as the Dallas location. If the connection between the Dallas and Memphis office were to go down, each site would be unable to access the information site stored at the other site. The Memphis site would lose all access to the internet as well as be unable to access internal E-mail. This same issue can arise due to the Memphis location only having a single router and single switch connected to the devices. If any piece in the line were to fail, the connection would fail as a result. Lastly, on the current network, the firewall only works to protect the network from outside connection through the internet. With how the firewall is currently used, it is unable to protect each device from internal threats or threats received through E-mail.

In summary, the network as it is currently designed suffers from many pitfalls. There is no redundancy put in place to prevent network failure if a component fails at the Memphis site. This could be addressed by utilizing multiple switches and routers at the locations to allow for back up connections to be made. The Memphis site’s internet connection is constantly suffering from the unnecessary path it must travel to connect to the internet. This could be resolved by implementing an internet connection at the Memphis site to prevent traffic from this site from needing to travel through the Dallas site. Lastly, better use of firewalls in needed. Each site should have their own respective firewall, on top of this, another firewall could be utilized to protect each server farm at each location. Threats can come from many locations, not just from the internet, this must be accounted for when designing and implementing a network.

**Physical Network Devices**:

The company network operates on the TCP/IP model for internet communication. “There are four layers of the TCP/IP model: network access, internet, transport, and application. Used together, these layers are a suite of protocols. The TCP/IP model passes data through these layers in a particular order when a user sends information, and then again in reverse order when the data is received” (Bodnar, 2021). The current network utilizes devices that operate on these different layers to work together to function seamlessly. The devices used by the company currently are Workstation Computers, Servers, Routers, Switches and Ethernet cabling. Functionally, these devices are all that is needed by the network. The Workstations fall into the layer 4 Application layer and act as the physical interface for the employees using the network. This is how the employees access the network, any data on the servers for various departments and e-mail, make calls (using VoIP, Voice over Internet Protocol) and use the internet. The physical network covers Layers 1,2 and 3, Network Access, Internet, and Transport layers respectively. The physical network is put together with a. combination of network switches, routers and ethernet cabling. In each location, Dallas and Memphis, the workstations and servers are connected via ethernet to network switches, two switches in Dallas and one switch in Memphis. These switches are connected via ethernet to the company routers, one router in Dallas and one router in Memphis. The Memphis router is connected via leased line ethernet to the Dallas router. The Dallas router functions as the internet gateway for the entire company network for both the Dallas and the Memphis locations. The Dallas router is firewall protected from the outside internet connection which is a leased line connection via ethernet.

Because the company is only using two routers, one in each location, the routers do not contain enough ports to connect all the devices to them. As such, the switches are necessary to allow all the employee workstations and the data servers to be connected to the routers allowing network access for these devices. The number of workstations and servers is less in the Memphis location, thus the reasoning for only one switch at that office. The Dallas office, being the bigger location, utilizes two switches to allow all the devices and servers to be connected to the network for use and access. In short, the switches connect to all the devices and allow them to be connected to the routers allowing them to gain network and internet access. Each connection between the devices is performed via ethernet cabling.

**Critical Traffic Patterns**:

According to the Wireshark traffic flow capture, a large majority of traffic on the company network comes via RTP protocol and SQL protocol traffic. This traffic translates to use of VoIP services and company application services. Based on the communication between source IP and destination IP, it appears that the VoIP traffic occurs between the Dallas and the Memphis office. This would make sense as the Memphis office houses the operations department of the company while the Dallas office is the main office with the most employees and devices on the network. The SQL application traffic comes from all the internal use of company systems. The operations department in Memphis appears to be in constant communication with the main office in Dallas resulting in the large amount of traffic shown on the Wireshark Capture. The other visible traffic on the network appears to be local on the network and could be attributed to the constant access of different local servers on the network. With the department servers being located on the network, this would account for the additional TCP traffic shown on the Wireshark Capture.

**Patterns Across the Infrastructure**:

The path network traffic must take depends on the originating location but follows a general guide for each office. From a workstation, a company utilizing VoIP software would send packets into the network over ethernet, into the switch the workstation is connected to and finally to the router of the office location. The router then will send the packet to the other office’s router which sends it into the switches and finally to the destination workstation. For traffic local to an office, such as an application accessing a server, the workstation sends packets to the connected switch, which will then send it to either the router, for forwarding to the switch the server is connected to, or forward directly to the server if it located on a port on the same switch.

**Performance Issues**:

The network as it is currently designed poses many issues for performance. The biggest pitfall of the network is the lack of redundancy and the impact of one component going down would have on the rest of the network. There are many possibilities for where performance issues can arise. The biggest issue is with the Dallas router. This router acts as the overall hub for the entire company network. Not only does it provide the internet access for the company network, it also serves to connect the two sites devices. If this main router were to go down, the entire network would fall apart and isolate each branch of the network from the rest. With this main router going down, each device would only be able to communicate with the other devices on the same switch that it is connected to.

The next performance pitfall comes from the way the entirety of the Memphis office is connected. This office has not internet connection of its own. As a result of this, it relies on the Dallas router for internet connection and must send all traffic through the leased line to the Dallas router before being sent out to the internet for acknowledgement. With the expansion of the network, this problem will be exacerbated by the addition of more workstations in the Memphis office. Effectively, by expanding the company, the traffic from the Memphis office will bog down the line connecting to the Dallas office and as a result can slow the connection for the Dallas office by overloading the Dallas router.

In the current state of the company network, growth of the company and expansion of the workforce will serve to slow the entire network if the network configuration is not addressed and resolved.

**Security Issues**:

The biggest security risk on the current network is that there is only a single firewall protecting the entire company network. While this firewall is placed to protect from the outside internet connection, it does nothing to prevent things once they are inside the network. There is a lot of important data stored on the servers at both sites. This data needs to be protected by itself. Another threat to the network comes from the potential for employees as well. Using an unauthorized device on the network poses a security risk. If an employee were to connect an unsecured flash drive to their work computer for any reason, it could upload a virus or malware onto the network allowing the malware a back door into the network and free reign of the system. This could also occur if an employee were to open an email with a phishing link or malware program attached. Overall, the way to network is setup leaves open many potential points of entry for attack of the network. “When a firewall sits between the Internet and users browsing the Web, that constitutes "client-protecting. t the other end of the spectrum is "server-protecting," which means that the firewall is protecting your servers from attack or infection. For example, a user who is intentionally or unintentionally saturating your Internet connection or the UTM firewall won't impact traffic to your e-commerce or websites if the connections and firewalls are separate. If something goes wrong and there's a denial-of-service attack against your web servers, which can slow or halt firewalls by filling session tables, then end-users will still be able to get their job done because their firewall won't be locked up. Conversely, if your end users become infected with a Trojan horse and their PCs are turned into attack machines, when they lock up their firewall, it won't affect incoming traffic to the server side of the house” (Snyder, 2009).

**Future Communications Needs**:

As the company looks to grow, its main form of communication will still be through VoIP phone services and company E-mail. To maintain the ability to stay in contact between sites, the company needs to look to increase the number of phones so that all employees have access to one. Additionally, the company needs to keep growth in mind and prepare as they progress to expand with offices in Kansas City and Houston. The biggest concern as the company grows would be the increase in congestion on the WAN due to increasing the number of users without changing the network design. In its current state, if the company continues with its planned employee expansion of 50% per year from the current 120 employees, the amount of bandwidth used by just the phone service alone will hinder the network bandwidth and cause problems. To prepare and resolve this issue, the company needs to provide the Memphis office with its own internet connection to prevent all traffic from traveling through the main Dallas location router. The same needs to be done when planning and installing the networks at the new regional offices once they come online. By doing this, it will take a large amount of congestion off the internal WAN and help alleviate stress on the network as the company expands.

With the same mindset, the company may do well to move the E-mail service from being operated on a local server at the Dallas office to a cloud-based service such as Microsoft Outlook. “The improvement in uptime enjoyed by cloud users provides a more efficient email experience than is enjoyed by workers at companies that still use internal email servers. When emails are sent and received through the cloud, there is greater availability and dependability than internal email servers. It is not unheard of for a cloud-based email service to be up and running 99% of the time or more” (Moving Email to the Cloud: Understanding Cloud-Based Email, 2020). The benefits of utilizing cloud-based E-mail also include scalability on demand, which is something the company is concerned with as they move forward with their expansion.

**Network Architecture**:

The future network recommendations can be viewed as a mirror of the company. The Dallas office serves as the Hub for the company, it is the main office. The Memphis office is a satellite office. The same goes when the future sites are created in Kansas City and Houston, they can be viewed as satellite offices. Understanding this we can translate it to a network design. The Dallas office will be the hub of the overall WAN with each office being satellites of the company network. Each office will be set up as their own LANs, they will each have their own stand-alone network to operate individually and prevent any issues between them if one LAN goes down, or as in the current network, if the hub goes down. All the offices together will encompass the company WAN. The WAN will be sub netted into local networks at each location and be connected to one another by a leased line internet service provider.

For the Dallas office, the router and switch setup will remain the same. The router will no longer be connected to the Memphis office, it will only provide internet access to the devices at the Dallas hub and be protected by a firewall to protect against outside access through the internet. Workstations will be connected to however many switches are needed to serve the number of workstations for employees. The switches are in place to connect as many devices as needed to the router as the router does not have enough ports to connect to the number of devices needed. Another switch will serve to connect the HR, Payroll and Accounting servers to the router and network. Each server will be protected by a firewall to serve as a redundancy to protect the company data from unauthorized access. Finally, video phones will be connected to a switch to connect to the network and utilize VoIP service to allow communications as needed, whether vocal or video, to conduct business and communicate between sites and departments.

The Memphis office will be set up like the Dallas office but on a smaller scale. The biggest change is that the Memphis office will be gaining its own internet connection. This is to prevent any problems associated with all internet traffic traveling through a single router at the hub location as well as to reduce bandwidth usage and network congestion all traveling through a single choke point on the WAN. The site will be set up with switches to connect workstations, video phones utilizing VoIP and servers. The Memphis servers are the Billing and Operations servers, and both will be protected by a secondary firewall to serve as a redundancy to protect the company data from unauthorized access.

The Kansas City and Houston offices, when they are ready to open, will mirror the Memphis office and have a network set up in similar fashion. The network can be expanded upon with the addition another router or more switches if needed. The addition of a router would be to alleviate traffic traveling through a single point at a given site. By operating 4 separate LANs to encompass the company WAN, traffic is managed at each site and directed in the easiest way possible to travel across the internet. All information stored on company servers is accessible from any site and will be protected by the implementation of multi factor authentication when company data needs to be accessed. This will be done to protect company data as well as work to prevent any data breaches as the company grows and expands into new markets.

**Planning and Security**:

The company needs to take action to make the changes to the network architecture quickly. The earlier this is done; the less back tracking will be needed with the company expanding. By addressing the issues and implementing the recommended changes sooner rather than later, the company can minimize the impact of the changes being made by doing it while the company is still small. Waiting until the expansion takes place, the company will be spending more money on a system overhaul and creating larger periods of downtime as the upgrades are done as opposed to the minimal impact the upgrades will have by performing them now and scaling the network alongside the expansion.

As the system is changed, a network management tool should be implemented to monitor the network. The recommended network management tool is SolarWinds Network Performance Monitor. “SolarWinds provides the Network Performance monitor that can reduce network outages and improve performance. It is a scalable solution with smarter scalability for large environments. It has functionalities for wireless network monitoring and management. It will allow you to view the performance metrics for autonomous access points. It has features for advanced alerting and auto-generating intelligent maps. For the critical network firewalls, switches, and load balancers, SolarWinds will provide a visual representation of performance” (Top 10 Best Network Monitoring Tools (2022 Rankings), 2022). The scalability of the SolarWinds tool along with its impactful features make it the best option for the company to adopt.

In terms of security, three types of security devices are recommended to be implemented as the system is overhauled. The first being the addition of more firewalls and outlined in the future network recommendations. This is done to better protect from multiple points of attacks and adds layers of redundancy to better protect company data. The second device is to establish multi factor authentication for employees when they log in to the network and access information. This is to aid in preventing unauthorized access to company data and keep anyone off the network that should not be on it. Finally, as the company is expanding, utilizing virtual machines on company computers. This is to server as another layer of protection redundancy. Another benefit of this is decreasing the impact of traffic flow on the network and keeping everything running smoothly.

The physical changes that need to be made to the network have already been discussed, the addition of multiple routers and switches to better support the company network will minimize the impact one office has on the others when experiencing issues. The changes to company computers will be the implementation of virtual machines. The company computers will need to be updated to change the operating systems and flash them into virtual machines. Doing this while before the company expansion will provide the smallest possible impact as any computers added in the future can be done before they are added to the company network.

To address the challenges, the company faces as they make changes to the network, it is recommended that a schedule be created to set a time for each computer to be updated. This will be done on a rolling schedule to make sure not all the computers are down at the same time. To upgrade the Memphis office and implement its own router set up, this will be performed on a weekend when the office is closed to prevent any impact on business and keep the office from being offline during business hours.

Failure to address the current network concerns and not keeping the system running optimally will impact company security. Company security standards need to remain consistently updated and a team needs to be in place to maintain this security. Failure to do so will put the company at risk of data breaches and outside interference.

# References

Bodnar, D. (2021, June 4). *What Is TCP/IP?* Retrieved from AVG: https://www.avg.com/en/signal/what-is-tcp-ip#:~:text=There%20are%20four%20layers%20of,when%20the%20data%20is%20received.

*Moving Email to the Cloud: Understanding Cloud-Based Email*. (2020, August 12). Retrieved from Frontier Business Products: https://www.fbponline.com/news/understanding-cloud-based-email/#:~:text=The%20improvement%20in%20uptime%20enjoyed,dependability%20than%20internal%20email%20servers.

Snyder, J. (2009, March). *How many firewalls do you need?* Retrieved from TechTarget: https://www.techtarget.com/searchsecurity/tip/How-many-firewalls-do-you-need

*Top 10 Best Network Monitoring Tools (2022 Rankings)*. (2022, May 4). Retrieved from Software Testing Help: https://www.softwaretestinghelp.com/network-monitoring-tools/