

SNHUEnergy: Network Assessment and Recommendation

Tyler J. Latshaw

Southern New Hampshire University

TABLE OF CONTENTS

EXECUTIVE SUMMARY	1
CURRENT NETWORK ARCHITECTURE	2
Critical Network Applications	2
OSI Model	2
Visual Representation	3
Physical Network Devices	3
Critical Traffic Patterns	4
Patterns Across the Infrastructure	5
Performance Issues	7
Security Issues	7
FUTURE COMMUNICATION NEEDS	9
Suggested Architecture Changes	10
Availability	10
Security	11
Scalability	12
Quality of Life	12
Visual Representation	13
PLANNING AND SECURITY	13
Mitigating Risk	13
Network Management	15
Implementing Security Devices	15
Changes to Existing Devices	16
Expected Challenges	16
Overall Risk	17
REFERENCES	19

CURRENT NETWORK ARCHITECTURE

Executive Summary

Based in Dallas, TX, SNHUEnergy is an up-and-coming oil and gas drilling company hoping to expand into refinement and transportation within the next two years. At the core of the company's operations is a network of various applications and hardware components that facilitate communication between the main office, the Memphis office, and future regional offices. The company's network consultant is tasked with evaluating the current network architecture, analyzing its structure, and making recommendations to ensure its success moving forward (Southern New Hampshire University, n.d.).

Based on the provided documentation and traffic flow captures, a large amount of the network's bandwidth is being consumed by audio and video telecommunication needs. This potentially could be resulting in slower speeds of more crucial applications such as payroll, accounting, or billing. Additionally, the network is not currently structured in an ideal architecture, nor is it suitable to be scaled larger as the company grows. Each satellite office is dependent solely on the Dallas office being online. If that office is inaccessible, all offices go offline, which could result in a loss of revenue and customer support. Moving forward, for the sake of reliability and security, the recommendation is to rearchitect the entire layout of the network, add additional devices and firewalls to ensure optimal security and reliability, and maintain the network in a manner that allows for positive growth in the future. The recommendations are documented in this report as follows.

CURRENT NETWORK ARCHITECTURE

Current Network Architecture

Critical Network Applications

Before evaluating the current network architecture, it is crucial to understand all of the applications that are reliant on the network, and by proxy, keep the business running from day to day. Their core functions distinctly structure the company's two offices; the Dallas office contains all HR and accounting functions, while the Memphis location handles billing and operations. Collectively, the current applications and services on the network consist of email, payroll, accounting, human resources, billing, operations, Voice-over-IP (VoIP), and video conferencing software (Southern New Hampshire University, n.d.).

OSI Model

From a broad level, the entire network in its current form can be adequately summarized using the Open Systems Interconnection (OSI) model. The model is used to standardize the way data and information flows through a network, regardless of the manufacturer. There are seven layers to the network, application, presentation, session, transport, network, data link, and physical (Cloudflare, 2019). From top to bottom, the data flows across the layers from the source and then back up the layers to the receiver.

For example, in the current network, a user in the Dallas office may want to connect to the billing application in the Memphis office. While this may take less than a second in real-time, it is a complex process. Using the OSI model, the request will originate from the end-user in the application layer when they open the application or click a button. The request is then prepared and encoded in the presentation layer before being passed to the session layer, where a new session is created between the user and the server. The transport layer takes the request and breaks it into segments to be transmitted. Once segmented, the network layer will then move the

CURRENT NETWORK ARCHITECTURE

data to the Memphis network, where the data link layer will move it within that new network.

The physical layer, the actual cabling, will convert the requesting data into binary for the server to consume, back through the model in reverse (Cloudflare, 2019). The server will, in turn, send the data back to the user in a similar manner.

Visual Representation

For a visual representation of the current network, see the attached documentation.

Physical Network Devices

At present, there are several physical network devices between the Dallas office, the Memphis office, and the entire network as a whole. These devices are collectively used in tandem to transmit both within and external to the network. Within the Dallas office headquarters, there is a firewall, a router, two switches, a Voice-over-IP (VoIP) phone system, a server farm, multiple wireless access points (WAP), end-user peripherals and devices, video conferencing software, and the company-owned computers. The Memphis office features similar elements on a smaller scale. Those devices include a single router and switch, a phone system, a server farm, end-user devices, video conferencing software, and company-owned computers. The Memphis office does not include a firewall or wireless access points. The specific function each device performs for the network is summarized in the following table.

Component	Office Location	Description
Firewall	Dallas Office	A critical security feature to filter both incoming and outgoing traffic to prevent malicious attacks
Router	Both Offices	A device that directs traffic between networks and the internet based on the shortest path
Switch	Both Offices	A device that connects multiple devices within the same network

CURRENT NETWORK ARCHITECTURE

VoIP (Voice over Internet Protocol)	Both Offices	A system for sending audio calls across the internet instead of a traditional phone line
Server	Both Offices	A centralized computer or group of computers that runs a specific application that other computers connect to
WAPs (Wireless Access Point)	Dallas Office	A device that smartphones, tablets, and computers can connect to for wireless internet
End Users	Both Offices	The employees' and guests' devices and computers
Video Conferencing	Both Offices	Devices such as cameras and speakerphones that allow users to meet virtually
Workstations	Both Offices	The computers that employees use to complete day to day operations

Table 1 This table created by the author highlights the various components within the SNHUEnergy network. Each component lists where the device is located, along with a brief description of what function it performs.

Critical Traffic Patterns

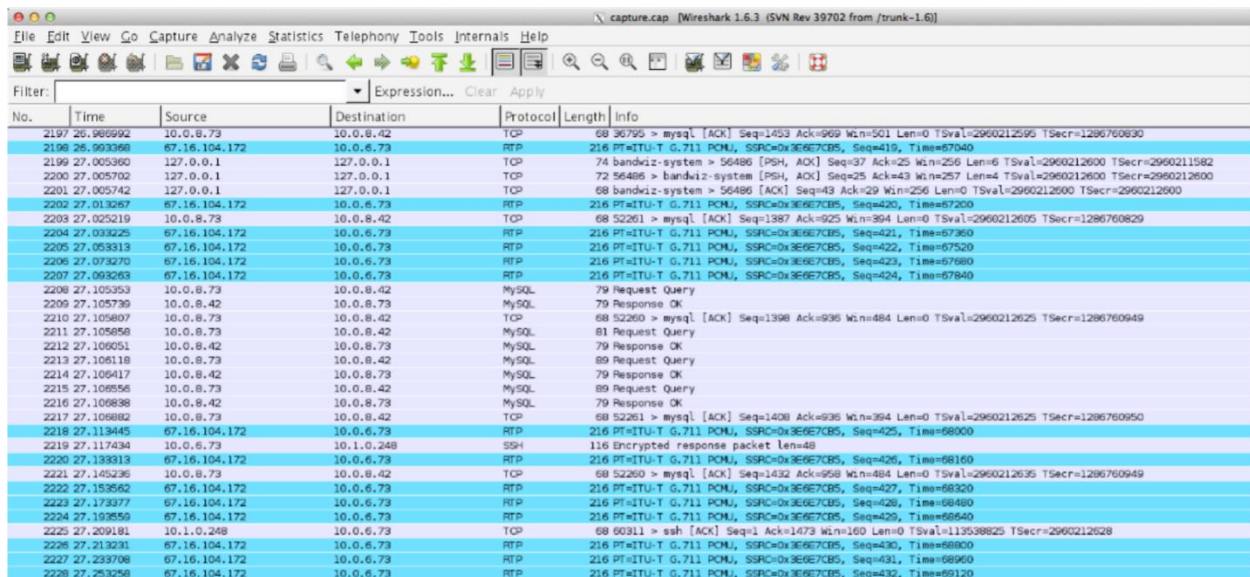
In order to properly evaluate and assess the traffic patterns within the SNHUEnergy network, it is important to look directly at a network protocol analyzer like Wireshark. Figure 1 below shows a sample output of the traffic noticed by Wireshark, which can be used to determine a few key factors about the network. First, based on the source and destination IP addresses, it can be noted that the company uses Internet Protocol version 4 (IPv4) standards for their network. This can also be validated against the network diagrams that have been provided. However, it is important to note that this is only a small subset of traffic and does not include any traffic from the Memphis office based on the IP addresses provided.

In addition to the IP addresses provided, the output shows that there are three main network protocols used for transmission. The protocols include transmission control protocol (TCP) for general data transfer, real-time protocol (RTP) for VoIP service data transfer, and MySQL for application-specific data. These three groups, VoIP services, application support,

CURRENT NETWORK ARCHITECTURE

and network management, make up the bulk of the traffic in the network. As mentioned, VoIP data transfer handles all of the audio and video that supports the phone system and video conferencing software. The application support transmissions support all of the physical applications that the employees are using in relation to the writing and retrieval to and from the databases. Lastly, transmission control protocol handles all of the general data transfer in the network typically not covered within these other two groupings.

Based on the console output in Wireshark, the network is also using user datagram protocol (UDP), but it is not explicitly shown in the protocol list in the network output. The network is also making use of secure shell protocol (SSH). SSH is used to transfer secure, encrypted data across the network when the company needs to ensure that the data remains safe and untampered. This could be used for data like customer information or credit card information if not encrypted in another way.



No.	Time	Source	Destination	Protocol	Length	Info
2197	26.966992	10.0.8.73	10.0.8.42	TCP	60	60 30755 > mysql [ACK] Seq=1453 Ack=936 Win=501 Len=0 TSval=2960212595 TSecr=1286760930
2198	26.993366	67.16.104.172	10.0.6.73	RTP	216	216 PtiITU-T 0.711 PCM, SSRC=0x3E6E7CB5, Seq=419, Time=67540
2199	27.005390	127.0.0.1	127.0.0.1	TCP	74	bandviz-system > 56486 [PSH, ACK] Seq=37 Ack=25 Win=256 Len=6 TSval=2960212600 TSecr=2960211582
2200	27.005702	127.0.0.1	127.0.0.1	TCP	72	56486 > bandviz-system [PSH, ACK] Seq=25 Ack=43 Win=257 Len=4 TSval=2960212600 TSecr=2960212600
2201	27.005742	127.0.0.1	127.0.0.1	TCP	68	bandviz-system > 56486 [ACK] Seq=43 Ack=29 Win=256 Len=0 TSval=2960212600 TSecr=2960212600
2202	27.013067	67.16.104.172	10.0.6.73	RTP	216	216 PtiITU-T 0.711 PCM, SSRC=0x3E6E7CB5, Seq=420, Time=67200
2203	27.025219	10.0.8.73	10.0.8.42	TCP	68	52261 > mysql [ACK] Seq=1387 Ack=925 Win=394 Len=0 TSval=2960212605 TSecr=1286760829
2204	27.033225	67.16.104.172	10.0.6.73	RTP	216	216 PtiITU-T 0.711 PCM, SSRC=0x3E6E7CB5, Seq=421, Time=67360
2205	27.053313	67.16.104.172	10.0.6.73	RTP	216	216 PtiITU-T 0.711 PCM, SSRC=0x3E6E7CB5, Seq=422, Time=67520
2206	27.073270	67.16.104.172	10.0.6.73	RTP	216	216 PtiITU-T 0.711 PCM, SSRC=0x3E6E7CB5, Seq=423, Time=67680
2207	27.093263	67.16.104.172	10.0.6.73	RTP	216	216 PtiITU-T 0.711 PCM, SSRC=0x3E6E7CB5, Seq=424, Time=67840
2208	27.105353	10.0.8.73	10.0.8.42	MySQL	79	Request Query
2209	27.105739	10.0.8.73	10.0.8.73	MySQL	79	Response OK
2210	27.105807	10.0.8.73	10.0.8.42	TCP	68	52260 > mysql [ACK] Seq=1398 Ack=936 Win=484 Len=0 TSval=2960212625 TSecr=1286760949
2211	27.105858	10.0.8.73	10.0.8.42	MySQL	81	Request Query
2212	27.106051	10.0.8.73	10.0.8.73	MySQL	79	Response OK
2213	27.106118	10.0.8.73	10.0.8.42	MySQL	89	Request Query
2214	27.106417	10.0.8.42	10.0.8.73	MySQL	79	Response OK
2215	27.106556	10.0.8.73	10.0.8.42	MySQL	89	Request Query
2216	27.106898	10.0.8.42	10.0.8.73	MySQL	79	Response OK
2217	27.106892	10.0.8.73	10.0.8.42	TCP	68	52261 > mysql [ACK] Seq=1408 Ack=936 Win=394 Len=0 TSval=2960212625 TSecr=1286760950
2218	27.113445	67.16.104.172	10.0.6.73	RTP	216	216 PtiITU-T 0.711 PCM, SSRC=0x3E6E7CB5, Seq=425, Time=68000
2219	27.117434	10.0.6.73	10.1.0.248	SSH	116	Encrypted response packet len=48
2220	27.133313	67.16.104.172	10.0.6.73	RTP	216	216 PtiITU-T 0.711 PCM, SSRC=0x3E6E7CB5, Seq=426, Time=68160
2221	27.145236	10.0.8.73	10.0.8.42	TCP	68	52260 > mysql [ACK] Seq=1432 Ack=958 Win=484 Len=0 TSval=2960212635 TSecr=1286760949
2222	27.153562	67.16.104.172	10.0.6.73	RTP	216	216 PtiITU-T 0.711 PCM, SSRC=0x3E6E7CB5, Seq=427, Time=68320
2223	27.173577	67.16.104.172	10.0.6.73	RTP	216	216 PtiITU-T 0.711 PCM, SSRC=0x3E6E7CB5, Seq=428, Time=68480
2224	27.193550	67.16.104.172	10.0.6.73	RTP	216	216 PtiITU-T 0.711 PCM, SSRC=0x3E6E7CB5, Seq=429, Time=68640
2225	27.209181	10.1.0.248	10.0.6.73	TCP	68	60311 > ssh [ACK] Seq=1 Ack=1473 Win=160 Len=0 TSval=113538825 TSecr=2960212628
2226	27.213231	67.16.104.172	10.0.6.73	RTP	216	216 PtiITU-T 0.711 PCM, SSRC=0x3E6E7CB5, Seq=430, Time=68800
2227	27.233708	67.16.104.172	10.0.6.73	RTP	216	216 PtiITU-T 0.711 PCM, SSRC=0x3E6E7CB5, Seq=431, Time=68960
2228	27.253258	67.16.104.172	10.0.6.73	RTP	216	216 PtiITU-T 0.711 PCM, SSRC=0x3E6E7CB5, Seq=432, Time=69120

Figure 1 This screenshot of the Wireshark application shows a sample of traffic flow through the SNHUEnergy network. Protocols shown include TCP, RTP, and MySQL (Southern New Hampshire University, n.d.).

Patterns Across the Infrastructure

Within the network, there are a number of critical applications that the staff makes use of on a daily basis, including email, payroll, accounting, and HR in the Dallas office and billing and

CURRENT NETWORK ARCHITECTURE

operations in the Memphis office. These are separate from the existing VoIP and video conferencing services already mentioned. The flow data to and from these applications takes in the network is fairly complex when compared to a user standpoint of just being able to click a button and receive the data needed. In actuality, data transfer takes many different paths to get from source to destination, albeit it is done extremely quickly.

Within the Dallas office, a request for data might originate from a corporate computer and then get transferred to switch 2. From there, the packet will be sent to switch 1 or to the router, which will then move it to switch 1. Once the request arrives at switch 1, it can be moved to the destination address at the server farm where the application is stored. The server will acknowledge the request and send data back through the system in a similar fashion but in reverse. Once the original source receives its data back, the application can give the requested information to the user. This process will continue as many times as needed in order to give the user all of the information they need.

A similar pattern can be seen within the network at the Memphis office. The main difference is that this office only has a single switch, so data from a corporate computer only needs to be sent to switch 1 and then directly to the server farm. All critical applications and other services will follow a similar pattern in either office. However, data transfer can become particularly complex when the source and destination addresses are in different office locations. For example, if a user in Memphis is requesting data housed in Dallas, the request would need to be sent to switch 1 in Memphis to the router which sends it to the Dallas office. From there, the request passes through the firewall for security checks and into the router. The Dallas router will route the request to either switch 1 or 2, which in turn will transmit it to the destination address. The data being sent to the other office will follow the same path back.

CURRENT NETWORK ARCHITECTURE

Performance Issues

Without seeing the full network logs or additional data, it can be hard to make any definitive conclusions on the network performance. However, a few assumptions can be made that might apply to SNHUEnergy. These performance concerns should be carefully evaluated prior to making any upgrades or expansions in preparation for additional offices. First and foremost, the Wireshark log shows that the company relies heavily on its phone and video systems, given the number of packets sent across the network. The main concern is that this could be slowing down the network given the bandwidth being consumed. Packets in the network using RTP are typically about 216 in length, whereas MySQL, SSH, and TCP are less than half of that between 68 and 116 in length at most.

Beyond this, it would be important to look at the actual hardware in the network as well and upgrade it as needed. It is not explicitly mentioned within the provided materials, but it can be assumed that the hardware is likely original or at least a few years old. While hardware can degrade over time, upgrading, in general, can warrant new features and faster speeds. For a business this size, they can expect to upgrade the wireless access points every five years, likely within two to three for best results, switches, and routers after five years, and the wiring between devices after ten years (Blalock, 2016). These changes should be made before expansion to mitigate any potential outages later on as there is inherently an existing chance for roadblocks when expanding a network. Getting the upgrades in place early on will allow the network engineers to check one less place for the cause of outage if one exists.

Security Issues

Similar to the performance, upgrading the network hardware can lead to key security upgrades as well (Blalock, 2016). As computer hackers become more advanced and creative with

CURRENT NETWORK ARCHITECTURE

their methodology, security software and hardware must keep up to remain ahead. It is important to note that a company does not always need to spend money on hardware upgrades in order to tighten security. Instead, the company can ensure that they are maintaining import software updates and patches as well as making sure that they configure the devices to their specific needs. However, most IT professionals agree that it is virtually impossible to overspend on network security, given how important it is (Blalock, 2016).

Looking at the network itself, the biggest security concern is that there is only a single firewall for all incoming and outgoing traffic from the Dallas office. While this can protect the office from attacks to that location, it does not fully protect the Memphis office. The company should immediately implement another firewall at the start of the Memphis office above the router. Since they are still connecting to the Dallas office through an Internet Service Provider (ISP), they are leaving themselves susceptible by not filtering their incoming data. At a minimum, each office moving forward should have a firewall directly after the ISP connection.

Given the information that the company stores in terms of billing and account information, it would also be advisable to have a firewall directly attached to the servers containing this information. It is not completely necessary, but it would help protect the information from any attack originating from within the network. This could be implemented before or after expansion as seen fit by the company. An example of this new architecture is shown as follows in Figure 2. While the company could add a separate firewall in front of each unique server, this is not necessary, nor is it fiscally responsible. It would be adequate for a single firewall to protect the server farm as a group pending the security features are adequate for the firewall they purchase. However, this would apply to both locations' servers, so Dallas would need a server-specific firewall, as would the Memphis office.

CURRENT NETWORK ARCHITECTURE

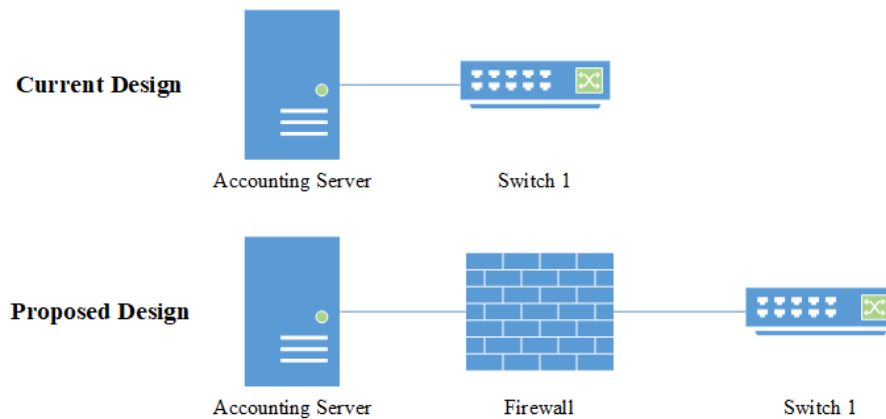


Figure 2 This diagram created by the author shows the current relationship between a server such as the accounting server and the switch that it is connected to. It is proposed to add a firewall between this connection so that the server is directly protected from security attacks.

Future Communication Needs

As previously mentioned, SNHUEnergy is looking to expand fairly significantly within the next two years by adding 50% more employees. This will take the employee count from about 120 to almost 200 employees. This will be completed by adding two additional offices in Kansas City and Houston. The overarching need for the company is simply having a network architecture that will support this growth and be ready to implement within the next year to a year and a half. The expectation is that the entire network and all of the offices be able to communicate with each other through the network adequately. While the two new offices will be smaller, regional offices compared to the headquarters in Dallas, they still need to be as reliable, similar to the other office in Memphis.

While the network is being reconfigured and reconstructed to support the two new regional offices, there are a few ideal characteristics that the new network will need to embody to meet the needs of the company. The network will need to first be scalable to meet the growth plans. Having a scalable network will mean that as the company grows, the network will be able to grow with it to complement it rather than hinder it. It is also expected that the network will remain reliable and accessible. Given the importance of the network to the company's operation,

CURRENT NETWORK ARCHITECTURE

it should not and cannot be unavailable to employees. Additionally, it will need to be more secure than it is now. During the analysis of the current network, it was determined that the network was not as secure as it could be. Lastly, the network and devices should be configured in a way that allows the system to be more proactive, all while being modernized to meet today's needs for the employees.

Suggested Architecture Changes

In order for SNHUEnergy's network to meet the needs of its upcoming growth, a number of significant changes need to be made to the current architecture. To facilitate these changes, they can be broken down and categorized into four separate characteristics – availability, security, scalability, and quality of life. Each of these categories is intertwined with the others meaning the overall success and performance are dependent on the changes whenever the company starts adding on additional employees and offices.

Availability

Given that the company will end up having four separate offices across the central United States, the primary focus of the changes will revolve around the network being available at all times. Currently, half of the servers are in the Dallas office, and the other half is in the Memphis office. Going forward, it would be suggested that the company build a data center into one of their offices, most likely the Dallas headquarters. Since all of the offices are consistently using all of the servers, it would make sense to move all of them into this new data center physically. Each of the locations will then connect with this area just as if they were connecting to one of the other offices. Without the data center, if one location were to go offline due to inefficient equipment, all offices would lose those servers. Since the company is likely on a budget, they

CURRENT NETWORK ARCHITECTURE

would be able to invest in enterprise-level hardware for just the data center instead of needing to do so for all four locations.

The data center will make use of two separate internet service provider (ISP) connections from different vendors so that if one connection were to go offline, it could immediately switch over to the other link. Likewise, if they need to perform any maintenance, they could easily pick which connection to use on-demand. On the office level, each of the locations each will have their own ISP connection as well. Currently, they would be connecting directly to the Dallas router, but it is reliant on the Dallas office being online. By moving to separate providers, they can ensure the availability of one location will not affect the others.

The last set of changes in terms of ensuring availability is regarding redundancy. Currently, regional offices like Memphis are only equipped with a single switch for the entire network. Moving forward, there will need to be a minimum of two switches per location, including the data center, for failovers. Hardware will fail from time to time, and they need to account for this. It is worth noting that ideally, there would be two identical data centers for complete redundancy in the event that one fails or has a power outage, but this is likely not realistic for a company of this size.

Security

Security is a significant concern in any network, let alone in today's world with all of the cyberattacks that are seen. Currently, SNHUEnergy only has a single firewall for its entire network. The firewall is responsible for filtering incoming and outgoing data to ensure that malware or other attempted attacks are not being passed through. Moving forward, it would be a requirement for every single location to have a firewall to protect it. It would be at the outermost area, right where the router connects to the ISP. Additionally, the data center will feature

CURRENT NETWORK ARCHITECTURE

firewalls for each of its two ISP connections. If allowed by the budget, additional firewalls will be placed directly connected to each server, or at least the ones with the most critical information, such as employee's personal information or customer credit card information. This would serve as another layer of protection if someone were to make it through the first firewall of the data center.

Scalability

It is vital for the network to be able to accommodate the two new offices being built, but it is also ideal for planning for the future. There may not be plans to add additional offices in a year, but that could change down the road. In the proposed network, each of the offices will have an identical architecture so that as the network expands, it will be easy enough for the IT department to mirror an existing office. This will also aid them in any maintenance as everything will be consistent and easy to memorize. Additionally, with the change to a data center instead of separate servers by location, they can ensure setting up a new office will be as simple as bridging the connection instead of needing to set up new servers and then go back to all of the other offices and then bridge those connections as well.

Quality of Life

It is great for the company to make all of the changes mentioned, but unless the network can support the speeds and throughput of all of the employees, it will all be for nothing as they would be no better off now. From an architectural standpoint, the main change would be moving all of the corporate computers in each office to a different subnet away from the video conferencing devices. Currently, the most extensive packets being sent through the network are from these devices, so moving the computers will help balance the load on the switches that they connect to. This will hopefully result in some speed gains.

CURRENT NETWORK ARCHITECTURE

Beyond this, SNHUEnergy needs to evaluate the current hardware in each office. For example, hardware and wiring can degrade over time (Blalock, 2016). The company should look to see if anything they have now should be updated to help with better speeds, or in the case of routers and switches, better features. The company should take this time to also include wireless access points (WAPs) in all offices so that employees can connect from anywhere in the office instead of just at their desks. This will go hand in hand with the final change, a better connection with the ISP. It is not explicitly stated what speeds they have now, but unless they upgraded in the past three or so years, they would likely be able to achieve better speeds from their ISP, such as gigabit internet.

Visual Representation

For a visual representation of the suggested future network, see the attached documentation.

Planning and Security

Given how much data is stored in a network today, it should be no surprise that security is one of the biggest concerns for any network architect. A network like SNHUEnergy's will hold not only sensitive customer information but also proprietary information that would be catastrophic for the business if it fell into the wrong hands or was made available to the public or competitors. In order to be at optimal performance and remain secure, the company will need to implement a number of changes before adding additional locations to the network.

Mitigating Risk

As previously mentioned, the company will need to start by creating a new, centrally located data center out of the Dallas office or another location depending on connections and physical space. The energy company will also work on adding a number of firewalls, unique ISP

CURRENT NETWORK ARCHITECTURE

connections, and additional wireless access points. However, it is important for SNHUEnergy to implement this new architecture in a specific order in order to mitigate as much risk and network unavailability as possible. Without doing so, the company risks data loss as well as customers and even its own staff from being able to access the network, which may result in a loss of revenue.

In general, it is recommended in this scenario for the company to begin staging the new data center and architecture alongside the existing network instead of performing it to the live version. This will allow them to properly test the setup and ensure that it is optimally working. Essentially, the team creating it will have two networks working concurrently, the current network and the new data center network. However, nothing will be patched into the data center at this point. Part of this will include creating backups of all of the servers and applications that are housed in the data center, as well as working with another service provider to add another ISP connection. Once it is up and running, they can begin installing additional firewalls to the newly added connections and servers.

Depending on the hours of the company, the final cutover for all of the offices will need to take place outside of normal business hours while there is as little traffic as possible on the network. This is likely on the weekend during the night. The network administrators will need to manually disable the network, perform any final changes to the physical architecture, and reboot the network so it can discover the new data center and additional devices such as switches and access points. By completing this during off-hours, they can avoid taking down the network in the middle of the workweek when demand is at its highest, ultimately mitigating risk to the performance and security.

CURRENT NETWORK ARCHITECTURE

Network Management

Once the company gets the entire network up and running, it is crucial for them to maintain it properly, or the entire effort will be for nothing. A common way to manage a network is through installing a network management tool. It is recommended to install an application like SolarWinds in order to monitor the network. The SolarWinds suite of applications consists of performance monitoring, traffic analyzing, configuration management, IP address management, device tracking, and more (SolarWinds, n.d.).

Given that the company is moving into additional locations and will start to see an increase in the number of devices and volume of traffic, this would be a beneficial addition for them. The network administrators would be able to monitor the network more passively and have it alert them for anomalies instead of waiting for outages to occur in order to fix them. Additionally, the new applications will help them properly manage and configure the network through IP addressing and device tracking. This is something that they currently do not have the ability to do.

Implementing Security Devices

Along with adding in the firewalls previously mentioned, there are a few other security devices that SNHUEnergy should install in order to make sure its newly reconstructed network remains secure. While the firewall will be the most impactful, they can also add a web filter in order to prevent or block users from accessing certain websites. The filter will restrict access based on the URL against a list of known phishing and malware domains (Melnick, 2019). By preventing access to these, the company can prevent a certain amount of associated risk. This can also be used to prevent access to inappropriate or mature websites as well as social media if the company desires.

CURRENT NETWORK ARCHITECTURE

Additionally, the administrators can install a network load balancer. This will likely only need to be implemented after the company grows more in size but can be useful to balance traffic. The balancer works by directing traffic and requests to different servers based on the desired configuration, essentially balancing out the requests (Melnick, 2019). This prevents one server from being overloaded with requests at any given time. However, using a load balancer does require having two or more servers for the same purpose; otherwise, all traffic would be going to the same server regardless of the balancer configuration. While a load balancer will mostly help with performance concerns, it can also help with the security concerns of a hacker trying to overload a specific server.

Changes to Existing Devices

Given the suggested architecture for the company, as they move forward, changes to any existing devices will remain mostly limited. The biggest change to hardware is the inclusion of additional routers and switches so that every location, including the data center, has at least two. This will not only help to balance out the traffic but will allow for a device to fall back on when the hardware fails in the future. Beyond this, the company will need to replace any outdated devices and cables to ensure they are performing at peak condition. They will also need to update any firmware to make sure they have the latest patches and features. Lastly, the network administrators will be reconfiguring the physical network topology slightly so that the VoIP devices are moved to a separate subnetwork away from the computers. This change will help alleviate some of the congestion for both sets of devices.

Expected Challenges

Implementing a new network or reconfiguring an existing one can be a daunting task and can present a series of challenges to the team completing the work. In this scenario, the biggest

CURRENT NETWORK ARCHITECTURE

challenge is the time needed to make the changes. The biggest way to mitigate risk is to gradually install the new data center to the existing network in a specific order of steps, as previously mentioned. By creating the new network in parallel with the existing one, they can progressively verify the performance of the system through testing the data center before fully moving all of the devices over. However, this does require some level of downtime for the network, but it can be completed during non-business hours to mitigate as much risk as possible.

Beyond this, there are a number of inherent challenges to overcome, including the preparation beforehand and then finally the management and maintenance of the network after the fact. Part of this will come down to trial and error of understanding the specific network and desired changes so that they know what not to do when implementing the changes. Depending on the team's experience, it may be helpful to document the entire process beforehand so that every employee involved fully understands the entire process and is prepared. This documentation can later be used to also help with the maintenance of the network.

Overall Risk

There is a significant risk associated with the current network if SNHUEnergy does not make changes to the architecture of the current network. The network is not designed to accommodate additional offices as they are all dependent on the Dallas office working correctly. If anything happens to that one location, every other office will also be affected, which is risky. Given the fact the company is expecting to add a significant number of employees and two new locations within the next two years, they will need to mitigate as much risk as possible beforehand as there is also a risk for failure when physically making the cutover to the new network.

CURRENT NETWORK ARCHITECTURE

The actual cutover to the network should be a smooth process, but inevitably things could go wrong. During the cutover, they might discover new issues that were never apparent, or a device might break in the process. The risk here is that they may not have backups readily available and will not be able to get them implemented in time for the business to resume operations. Once it is up and running, there is an additional risk associated with not properly maintaining the network. The team needs to ensure that they are constantly monitoring the network for threats as well as keeping its security services up to date. By not doing so, they are opening the company up for potential hackers and intruders, but by not reconfiguring the network at all, the risk is much more significant. In comparison, the risk of cutting over and maintaining it is much less and will ultimately be worth it for the employees and the company in the long run.

CURRENT NETWORK ARCHITECTURE

References

Blalock, J. (2016, March 24). *How Often Should I Replace my Networking Devices*.

Hummingbird Networks. <https://info.hummingbirdnetworks.com/blog/how-often-should-i-replace-my-networking-devices>

Cloudflare. (n.d.). What is the OSI Model? Cloudflare; Cloudflare, Inc. Retrieved July 11, 2021, from <https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/>

Melnick, J. (2019, January 22). Network Security Devices You Need to Know About. Netwrix; Netwrix Corporation. <https://blog.netwrix.com/2019/01/22/network-security-devices-you-need-to-know-about/>

SolarWinds. (n.d.). SolarWinds Network Management Licensed Products. SolarWinds; SolarWinds Worldwide, LLC. Retrieved July 11, 2021, from <https://www.solarwinds.com/network-management-software>

Southern New Hampshire University. (n.d.). *IT 640 Final Project Scenario*. Retrieved May 30, 2021, from http://snhu-media.snhu.edu/files/course_repository/graduate/it/it640/it640_final_project_scenario.pdf