SNHUEnergy, Inc: Network Analysis, Recommendations, and Expansion Plans

Ivan Novasak

Southern New Hampshire University

IT 640: Telecommunications/Networking

Corley Hughes

2024 April 28

# SNHUEnergy, Inc: Network Analysis, Recommendations, and Expansion Plans

The purpose of this document is to lay out SNHUEnergy, Inc.’s current network with branches in Dallas and Memphis, any issues it may have, as well as prepare staff for what needs to be considered for an expansion to Kansas City and Houston (Hughes, 2024e). To be covered is:

* The current network architecture;
* The network devices and where they fit in the OSI model;
* The purpose and description of each hardware component;
* Graphical diagrams of both the current and possible future network designs;
* Traffic patterns;
* Analysis of the current network to determine any performance, reliability, or security issues;
* Suggested changes;
* Planning the new network for performance and better security;
* The risks of not making the changes from security and reliability perspectives.

# Executive Summary

An analysis was conducted on SNHUEnergy, Inc.’s current network in the Dallas and Memphis offices and several recommendations have been given that will make the network faster, more secure from malicious threats, as well as more reliable in the face of natural disaster in preparation for expansion to the 2 new sites in Kansas City and Houston. These changes include:

* Having each office have 2 Internet Service Providers (ISPs): a primary and a secondary;
* Dividing each office’s internal network into multiple networks that will prioritise certain devices, such as IP phones and the servers, as well as segment different devices so that if a component fails, the rest of the network will still continue to function;
* Recommendations of security policies that prevent malicious access both from the outside from network attacks as well as from internal social engineering attacks;
* Description of all required network components as well as their prices for parts and labour for installation of the new networks.

**Current Network Architecture**

**Network Applications**

There exist 3 diagrams that show off how the current network looks: the Organizational Network Diagram, Dallas Office Network Diagram, and the Memphis Office Network Diagram (Hughes, 2024a/b/c). The Organizational Network Diagram shows the overall network of the company and how each office is linked to each other as well as the Internet (Hughes, 2024a). The 2 Office Network Diagrams show the network setup for each individual office (Hughes, 2024b/c).

The Organizational Network Diagram is first to consider. In the diagram there are graphics for each component as well as the offices, and a listing of network components (Hughes, 2024a). The Dallas portion of the graphic shows computer servers for HR, Payroll, E-Mail, and Accounting; 2 switches; 1 router; 1 firewall; 3 workstations; and 2 network links: 1 from the firewall to the Internet and the other form the router to a router at the Memphis office. The Memphis portion of the graphic shows 1 router; 1 switch; 3 workstations; computer servers for Billing and Operations; as well as a network link from the router to one of the Dallas office routers. Also stated in this diagram is some more information about each office in boxes near the bottom of this diagram. For the Dallas office, it is stated that there are 90 employees; applications for E-Mail, Payroll, Accounting, and HR (shown as servers in the graphic); hardware of 1 router, 2 switches, and 1 firewall; and connectivity to the Internet (Hughes, 2024a). For the Memphis office, this information is listed as 30 employees; applications for Billing and Operations (shown as servers in the graphic); services for a VoIP Phone System (not shown) and video conferencing (not shown); hardware of 1 router, 1 switch, 0 firewalls; and connectivity to the Internet.

The Dallas Office Network Diagram (Hughes, 2024b) is next to consider. This diagram shows a set of IP phones, a server farm, and wireless access points connected to a switch labelled Switch-1; a set of end-users, a set of video conferencing cameras, and a set of corporate computers connected to a second switch that is labelled Switch-2; and those 2 switches are connected to each other as well as a router. That router is connected to a firewall which, in turn, is connected to the Internet by whatever means the ISP is using (not indicated in the diagram).

The final diagram to consider is the Memphis Office Network Diagram (Hughes, 2024c). This diagram shows a set of IP phones, a server farm, a set of end-users, a set of video conferencing cameras, and a set of corporate computers each connected to a switch which, in turn, is connected to a router, and that router is connected to the Dallas office via whatever means of connectivity is being used (not indicated in the diagram).

The types of networks in force for SNHUEnergy, Inc. appear to be a Wide Area Network (WAN) for the connection between the Dallas and Memphis offices, a local area network (LAN) within each office to provide a connection between all of the physical hardware components, a wireless local area network (WLAN) for the wireless access points (WAPs) in the Dallas office, a storage area network (SAN) for each of the server farms each office has, and possibly personal area networks (PANs) for the connections between the IP phones and their base stations, if those phones are cordless (uCertify, n.d., p 16; Darah, 2022).

**OSI Model Identification and Label**

This section of the document is for identifying which hardware components and connections in the current network are in the most appropriate layer(s) of the Open Systems Interconnection (OSI) model. Table 1, shown below, lists the OSI layers and the respective appropriate network components.

**Table 1**

**OSI Layers and Network Hardware**

| OSI Layer | Hardware Component(s) |
| --- | --- |
| 1: Physical | Ethernet cables, fibre-optic/coaxial/other cable connecting to ISP-issued hardware, radio waves, WAPs |
| 2: Data Link | Switches, network interface cards (in computers), WAPs |
| 3: Network | Routers |
| 4: Transport | Firewalls |
| 5: Session | Firewalls, PCs |
| 6: Presentation | Firewalls, PCs |
| 7: Application | Firewalls, PCs, Servers, IP Phones, Webcams |

*Note*: Indexing of hardware components to OSI layers is based on (Darah, 2022; English, 2022; GeeksforGeeks, 2022; Shahid, 2022; Shaw, 2024; uCertify, n.d.).

**Hardware Components Description**

This portion of the document is for outlining the functions of each hardware component in the network. A listing follows showing each component and its function(s):

* Cabling: Cables are used to connect devices together in formation of a physical network (GeeksforGeeks, 2022; uCertify, n.d., pp 27–29). They may be Ethernet, fibre-optic, coaxial, twisted-pair, or another style of cable. Cables are vital to any computer network and will be needed at a minimum of 1 point along a network.
* Switches: Forward data from one device to another based on the MAC address of the incoming data frame (GeeksforGeeks, 2022). The data gets sent to the specific Ethernet port on the switch the other device is connected to, based on the MAC address table the switch has (English, 2022). These devices aren’t essential for every type of network as they are mainly used to interconnect devices within a single LAN, whereas routers, mentioned below, are essential as they are required to interconnect 2 different networks (including connecting devices to the Internet) (Cloudflare, n.d.). SNHUEnergy, Inc. has a network that is large enough to benefit from switches and is using them.
* Wireless Access Points (WAP): Interconnects devices to a LAN wirelessly (uCertify, n.d., p 106). These allow smaller, battery-powered, mobile devices such as laptop computers, smartphones, and tablets to gain connectivity to the Internet and other computer networks via Wi-Fi, which uses radio waves at the 2.4 GHz, 5.8 GHz, and 6 GHz frequency bands (Kelly, 2022; uCertify, n.d., p 106). The distance the signal can travel is up to 250 (uCertify, n.d., p 106) to 300 (Kelly, 2022) metres. Without these, all devices would require physical cabling to be networked.
* Network Interface Cards (NICs): Provide the physical connection between a computer and a network, typically using an Ethernet cable or a wireless antenna but some cards also can use fibre-optic cables or USB for the network interconnect (John, 2023; TechTarget Contributor, 2023). These are also known as a network interface controller, network adapter, or a LAN adapter (John, 2023; TechTarget Contributor, 2023). Without a NIC, a device can not access the Internet or another computer network.
* Routers: Connect networks to each other and forward data packets between the networks based on their destination IP addresses (English, 2022; GeekforGeeks, 2022; uCertify, n.d., p 7). Routers are required for linking an internal network (say, a home, school, or company network) to the wider Internet or a second network (English, 2022; GeekforGeeks, 2022; uCertify, n.d., p 7).
* Firewalls: Filter data packets travelling into and out of the network for detection of and blocking security vulnerabilities and hackers (Fortinet, n.d.; Yasar & Lutkevich, 2023). They are instrumental in keeping private data from the internal network out of malicious hands. Another functionality of a firewall is prevention of users on the network from accessing unauthorised websites, such as a school network that needs to prevent people at the school from visiting pornography websites (Fortinet, n.d.; Yasar & Lutkevich, 2023). Not having a firewall is putting one’s network at risk of cyber attacks and so it’s never logical to go without this component.
* Servers: These provide data and services to other computers and their users, known as clients, on the network (Posey, 2021). The hardware between servers and desktop computers is similar though servers have a much higher volume of memory, that is also error-correcting, to handle the high number of requests coming from users and their computers (Posey, 2021). These are essential for handling large volumes of data as found in any large corporation’s operations.
* VoIP Phones: These are similar to regular analogue telephones but run on a computer network and may be in either physical hardware form or available as a software application on computers (Chai, 2021). VoIP phones may offer additional features not available on analogue phones such as video calls, instant messaging, Internet fax, voicemail with text transcription, Bluetooth headset connectivity, and mobile & local number portability that allows the customer to retain their existing phone number while switching carriers (Chai, 2021). One word of warning, though: some VoIP phones do not offer emergency call support, so one needs a cellular phone to call for emergencies (Chai, 2021). Check to make sure the one being bought supports ‘E-911’ if using it in the US (Chai, 2021).
* Webcams: Used for video conferencing. These may be separate devices or built into the user’s desktop or laptop computers (Chai & Lazar, 2021). The ability to do video conferencing is essential as it helps to put a face to the company or organisation customers and members are interacting with. Video conferencing has become especially popular since early 2020 when the COVID-19 pandemic began and forced social distancing rules into force (Chai & Lazar, 2021).

**Network Devices in Use at Each Branch Office**

According to Hughes (2024a/b/c), the breakdown of network devices by location is as follows:

Dallas Office Network (90 employees):

* Multiple IP Phones;
* 4 servers for payroll, accounting, e-mail, and human resources (HR);
* Multiple Wireless Access Points (WAPs);
* Corporate workstation computers;
* Multiple webcams for video conferencing;
* End-users’ client computers/other devices;
* 2 switches;
* 1 router;
* 1 firewall;
* Cabling to connect the wired hardware components;
* WAN link to ISP.

Memphis Office Network (30 employees):

* Multiple IP Phones;
* 2 servers for billing and operations;
* Multiple webcams for video conferencing;
* Corporate workstation computers;
* End-users’ client computers/other devices;
* 1 switch;
* 1 router;
* Cabling to connect the wired hardware components;
* WAN link to Dallas office network.

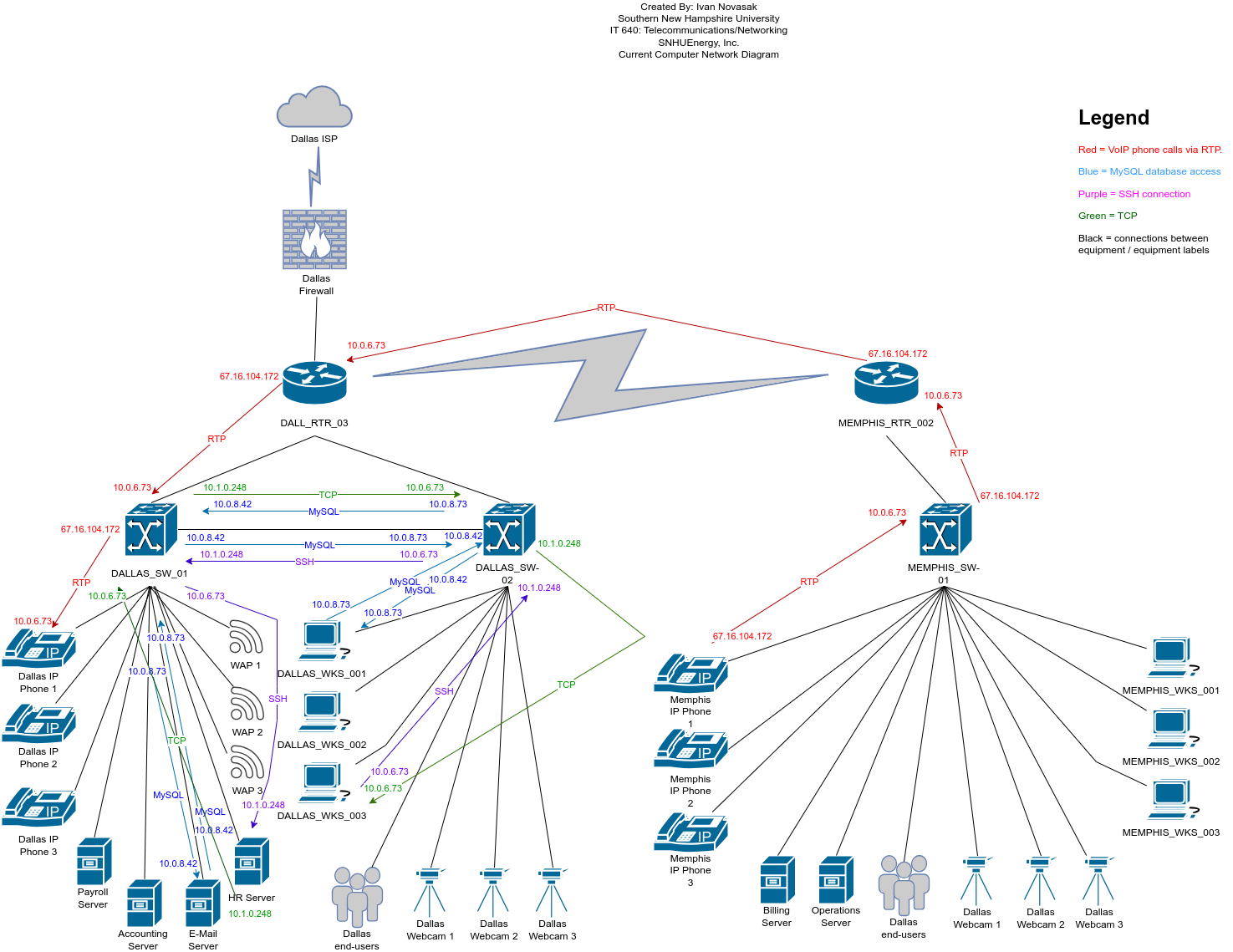
The functionality of each of these devices was already covered in detail in the Hardware Components Description section of this document. As a recap, the switches are for devices to communicate with each other on the same network, the routers are for linking networks together so services can communicate beyond their network, the firewall is for blocking malicious network traffic, the WAPs allow employees and end-users to be mobile across the company, and the WAN links are for connecting our company’s networks to the Internet (Novasak, 2024, pp 2–7).

**Visual Representation**

Figure A-1, shown below, shows a diagram of the current network and traffic described in the Traffic Patterns sections of this document.

**Figure A-1**

Current SNHUEnergy, Inc. Network



*Note*: Adapted from Hughes (2024a/b/c).

**Initial Network Analysis**

After looking over the diagrams, the author makes the following observations:

1. The Dallas portion of the network appears to be fine, having a firewall as protection between network and the outside world (ISP), as well as 2 switches to balance the traffic around the network (Hughes, 2024b).
2. The Memphis portion of the network looks pretty different to the Dallas portion. This portion of the network has the VoIP phones, servers, end-users, webcams, and desktop computers all connected to a single switch, and that switch is connected to a router, which, in turn is connected to the router at the Dallas office (Hughes, 2024c). The first observation the author notices is the lack of a firewall between 2 routers. If any malicious data or code were present in either the Dallas or Memphis networks, it could move around the network due to the firewall only protecting against data from the wider Internet getting into the Dallas network (Hughes, 2024a). Having everything connected through a single switch or router like in this Memphis case could result in the entire Memphis office being unable to run should that switch or router have a problem functioning. A single point of failure is never a good thing to have in a network.
3. A third observation the author notices is that the network appears to be hierarchical in nature, with only the Dallas portion having direct access to the Internet (Hughes, 2024a). If there were a problem at the Dallas office that prevented the office from connecting to the Internet (say, a freak snowstorm and deep freeze like in February 2021 that caused widespread power outages across Texas), the Memphis office would also have no connectivity to the Internet due to all of its data having to be routed through Dallas first. This would result in the Memphis office not having connectivity to the payroll, E-mail, HR, or account data that are stored at the Dallas office. Also, the Dallas office network would not be able to access the billing or operations data which are stored in the Memphis office.

**Critical Traffic Patterns**

According to the *SNHUEnergy Inc. - Traffic Flow Wireshark Capture* (Hughes, 2024d) screenshot, the following IP addresses are identified as communicating with each other:

* 10.0.8.73;
* 10.0.8.42;
* 67.16.104.172;
* 10.0.6.73;
* 127.0.0.1;
* 10.1.0.248.

In addition, the following protocols were in use:

* Transmission Control Protocol (TCP);
* Real-time Transport Protocol (RTP);
* Structured Query Language (MySQL);
* Secure Shell (SSH).

According to Kinza Yasar and Ben Lutkevich, of TechTarget, TCP is the main standard used in networking / the Internet by which devices and applications transfer data to each other by breaking data up into packets that get disassembled, transported around the network, and reassembled at the destination (Yasar & Lutkevich, 2023). Without it, other protocols and applications like SSH, Voice over IP (VoIP), e-mail, databases, video conferencing, and web pages would not be possible (Yasar & Lutkevich, 2023). TCP ensures all packets arrive intact via acknowledgement signals that get sent from the destination device back to the source device every time packets are sent (Yasar & Lutkevich, 2023). Everything else in the network depends on the existence of TCP (Yasar & Lutkevich, 2023).

According to Chiradeep BasuMallick, a technical writer at Spiceworks, Inc., RTP is used in conjunction with the User Datagram Protocol (UDP) and is part of the TCP/IP architecture for audio and video streaming/conferencing as well as VoIP phone calls (BasuMallick, 2022). The protocol has error correction, sequencing, and synchronisation to ensure the packets come in the correct order so the audio or video does not arrive in a jumbled form (BasuMallick, 2022).

According to Ravikiran A S, of Simplilearn Americas Inc., SQL is a scripting language used to create and manage relational database systems (Ravikiran, 2023). It is also used for ‘retrieving, adding, or manipulating data’ in database systems (Ravikiran, 2023). MySQL is an open source relational database management system (RDBMS) that was created in 1995 by MySQL AB and later acquired by Sun Microsystems, who are now part of Oracle Corporation (Ravikiran, 2023). A relational database is a system for storing and managing data across organisations and companies that uses tables that ensures data integrity and consistency (Ravikiran, 2023). The relations between those tables are what make the database a relational database (Ravikiran, 2023). MySQL is how one manipulates the database via either command line or a GUI application (Ravikiran, 2023).

According to Chip, of QuantHub, the 5 components of a relational database are tables, columns, rows, primary keys, and foreign keys (Chip, 2023). Tables are used to store data about particular types of entities in the database (Chip, 2023). They are usually given names like Customers, Vehicles, Employees, Products, etc. (Chip, 2023). Within tables, there are columns, or attributes, which are specific types of data, such as an employee’s first name, last name, date of birth, address, or ID number (Chip, 2023). Next are rows, or records, each of which represents one full entry in a specific table (Chip, 2023). In an Employees table, each row would represent an employee (Chip, 2023). A primary key is a table’s attribute that is unique for every row and is used for linking to other tables (Chip, 2023). A foreign key is used to link tables in the database together via the table’s primary key (Chip, 2023).

According to Cloudflare, SSH is used when someone needs to use one computer to communicate with another computer remotely over an encrypted connection (Cloudflare, n.d.). It is usually used when an administrator or manager needs to access a server and they are not on-site to do it directly (Cloudflare, n.d.). SSH is used via TCP port #22 and can bypass the firewall if the firewall is configured to allow connections through port #22 (Cloudflare, n.d.). Another purpose for SSH is port forwarding, which is where data that normally goes through one port is instead redirected to go over another port (Cloudflare, n.d.). According to Peter Loshin and Michael Cobb, of TechTarget, SSH was developed by Tatu Ylönen in 1995 when they were a researcher at Helsinki University of Technology (Loshin & Cobb, 2021).

**Traffic Patterns Across the Infrastructure**

Priyanka Shyam, writing for LinkedIn, states that IPv4 addresses are grouped up into Classes A, B, C, D, and E, with the first 3 decimal digits (‘octet’) determining which of these Classes a particular IP address belongs in (Shyam, 2019). The arrangement is as follows:

* Class A has the first octet of 0–127;
* Class B has the first octet of 128–191;
* Class C has the first octet of 192–223;
* Class D has the first octet of 224–239;
* Class E has the first octet of 240–255.

She also states that the respective subnet masks for Classes A, B, and C are 8, 16, and 24, respectively (Shyam, 2019). The IP addresses shown in Hughes (2024d) appear to be Class A addresses, as their first octet falls within the 0–127 range (Shyam, 2019). Shyam also states that for Class A IP addresses, the first octet is the network portion of the IP address, with the remainder of it being the host part (Shyam, 2019). She states that the subnet mask is combined with the IP address to determine which network the device is on (Shyam, 2019). Unfortunately, no subnet masks were shown in Hughes (2024d), but since these IP addresses are all Class A, and devices on the same network will share the first octet of the IP address, it can be decided that the IP addresses in the screenshot with 10.x.x.x are on 1 network and 67.x.x.x is on another network (Shyam, 2019). IP addresses starting with 127.x.x.x are special IP addresses called loopbacks (Shyam, 2019). According to Sofija Simic, a technical writer at phoenixNAP, the IP address 127.0.0.1 is a popular IP address used to refer to the computer one is working on (Simic, 2023). It is also known as localhost (Simic, 2023). It is typically used for blocking websites, testing apps and programs, and hosting apps locally (Simic, 2023). It is much faster when needing an app to function that doesn’t really need a network connection, like when a networked app is being tested and a simulation of a network connection is needed (Simic, 2023).

After examining the screenshot by Hughes (2024d), the following observations can be noted:

1. A VoIP phone call between the networks 67.16.104.72 (the source) and 10.0.6.73 (the destination) using the G.711 codec over RTP which, according to Snom Technology, delivers 8 KHz sample rate audio quality (Snom, n.d.);
2. Next comes a series of TCP and MySQL connections between 10.0.8.73 and 10.0.8.42, with these IP addresses swapping source and destination many times. Since MySQL is used to manage relational databases, these entries are likely from someone updating the database due to information they received over the phone call just prior.
3. Finally, the phone call between 67.16.104.72 and 10.0.6.73 resumes and simultaneously, an SSH connection is opened with a source IP address 10.0.6.73 and a destination IP address 10.1.0.248. During the phone call, destination IP from the SSH is used as a source in a later TCP connection between 10.1.0.248 and the destination 10.0.6.73 (the same destination that is in the phone call). Perhaps the SSH connection could be a manager remotely verifying something the callers did earlier in the database via MySQL.

**Performance Issues**

Some key observations were noticed and pointed out in (Novasak, 2024) regarding the network: mainly that the entire company - both branches - were running on a single Internet connection. In addition, the Memphis branch had only 1 router and 1 switch that all devices connected through (Novasak, 2024).

Regarding Internet connections, according to QuoStar in the article entitled *Why your business needs two Internet connections*, Internet outages cost businesses in the UK £7 billion in 2016 alone, with businesses having an average of 4.7 outages per year with each costing the business £3,644 on average (QuoStar, 2019). QuoStar goes on to mention 3 types of Internet connections businesses may use: broadband, leased line, and 4G (mobile). They state that broadband is typical for home connections and bandwidth is shared with other customers, which leads to lower performance at peak times and performance that fluctuates (QuoStar, 2019). QuoStar states that leased line is good for growing and medium-sized businesses and is necessary for large companies (QuoStar, 2019). It is a private connection which only the subscriber can utilise and so doesn’t have the performance fluctuations that come with shared broadband bandwidth (QuoStar, 2019). Finally there is 4G, which QuoStar states may be good for satellite offices or remote locations far from fixed lines but are typically not enough for full business operation and so are better only as a lifeline in case the main connection fails (QuoStar, 2019). Given that SNHUEnergy is expanding, it makes sense now to look into getting each location upgraded to a leased line for the primary Internet connections and consider 4G/5G or a second ISP in the area for a backup connection in case the main connection fails. Rural Telecommunications of America states in an article entitled *Benefits of having multiple web connections for businesses*, that the advantages of having more than one Internet connection include (RTA, n.d.):

* increased reliability;
* improved network performance (especially when using load-balancing to distribute the network traffic over the different connections);
* better network security against cyber criminals and data breaches (so if one connection is compromised, the other one can still be safely used);
* flexibility to choose the right connection when a business is going to be expanding and adapting to changing requirements (RTA, n.d.).

According to Deepesh Sharma in his MakeUseOf article entitled *Should You Use More Than One Router? The Pros and Cons*, there are 5 advantages of using multiple routers in a network (Sharma, 2022):

1. Extended wireless range and more capacity due to both routers being able to share the network’s users, so no single router will be overloaded due to a sudden influx of a lot of users;
2. Enhanced security by having multiple networks: when a second router is used, the first router’s connected devices are visible to it but not the other way around, so the devices connected to the second router are more secure (Sharma, 2022).
3. Compartmentalisation of networked devices: since devices connected to the second router are not visible to the devices connected to the first router, it makes sense to connect devices that have more security vulnerabilities to the second router, where they will be isolated from the wider network (Sharma, 2022).
4. Less downtime: should a router have a problem, having a second router in place allows traffic to continue to flow in the network via the second router, enabling the business to continue operations while the defective router is getting replaced (Sharma, 2022).
5. More Ethernet ports allowing for more wired devices: having a second router allows for more wired connections and allows one to free up valuable Wi-Fi frequency spectrum in the network for devices that can not be connected via physical cables (Sharma, 2022).

**Security Issues**

According to a 2021 article entitled *3 Top Risks of Not Having a Firewall*, Mark Sheldon Villanueva, of Intelligent Technical Solutions, states that the top 3 risks businesses take on when not having a firewall are (Villanueva, 2021):

1. Unlimited public access to the business’s private network, including by hackers and other malicious actors who are out to steal data;
2. Data breaches, which have cost businesses an average of $4.24 million per incident as of 2021, which was up from an average cost of $3.85 million per incident in 2020 (Villanueva, 2021). Hackers may hold a business’s data for ransom, threaten to leak it publicly, or delete it (Villanueva, 2021). Any of these can lead to failure of a company or organisation (Villanueva, 2021).
3. Unplanned downtime or network collapse: not having a firewall would allow cyber criminals who come across the network to cause such damage that business can take on losses as high as $25,000/*minute*, which is a amount that can cause business failure if this type of loss is sustained over a long enough period of time (Villanueva, 2021).

**Future Network Architecture**

In Novasak (2024b), *SNHUEnergy, Inc: Current Network Architecture* (also in the previous section on this document), the architecture of the current network including its devices, current traffic flows, and a diagram were presented to show how the network was functioning. Also, the issues with having only 1 switch and router as well as no dedicated Internet connection in the Memphis office were discussed. This portion of the report, *Future Network Architecture*, will attempt to remedy these issues to enhance the existing network and prepare for the SNHUEnergy’s expansion into Kansas City and Houston (Hughes, 2024e).

# Future Communication Needs

After examining the diagrams in Hughes (2024a/b/c), the first observations are the end-user devices that exist equally on both networks. These will likely be required at the new offices as well. So one can expect to need more workstations, IP phones, and webcams. This is because the people at the new offices will need to communicate with people at the existing offices. A similar number of back-end devices will also be needed to get the new locations online. These devices include switches, routers, firewalls, wireless access points, cabling, and links to the ISP.

**New Network Architecture**

Some suggestions of new devices in the network follow, with a similar setup expected for Kansas City’s and Houston’s networks.

* Have more than 1 switch in the Memphis network so that there is room for more connections;
* Add a dedicated ISP link to the Memphis network so people at the Memphis office are not affected by any events that could take the Dallas network offline;
* Add wireless access points into the Memphis network, and have these in all future locations, as well;
* Add a firewall into the Memphis network to protect it from malware coming in or leaving that office;
* Tentative: have a switch for each type of device (webcams, workstations, servers, WAPs, VoIP phones, end-user hardware, etc), which will allow for plenty of room for hardware expansion;
* Tentative: have separate networks for back-end internal hardware and devices people interact with.

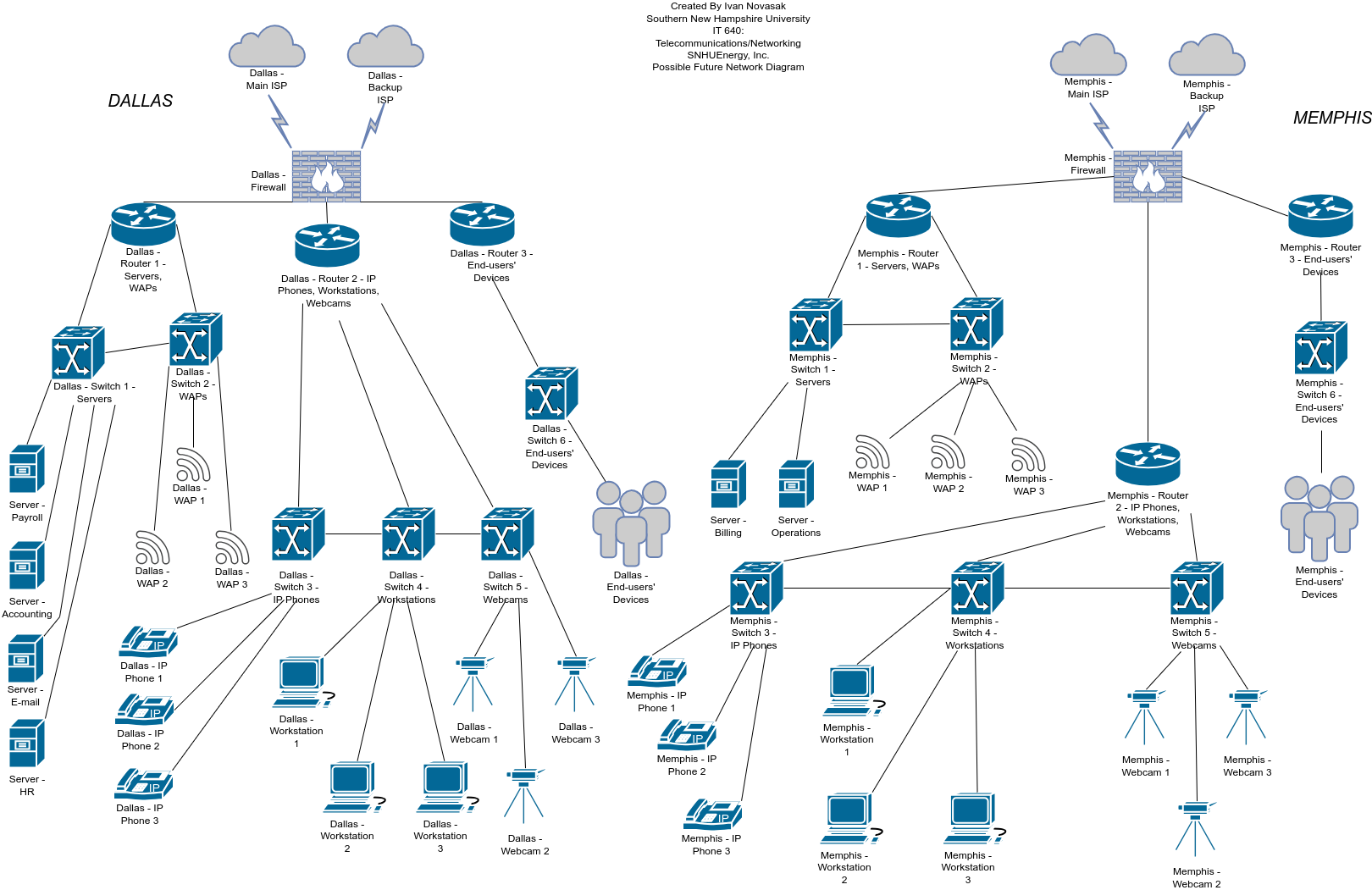
**New Network Visual Representations**

***Dallas and Memphis***

In Figure B-1, shown below, is the tentative future network showing the modifications for the Dallas and Memphis networks. A consideration is whether to totally isolate different hardware categories into different networks or if they should be able to connect to each other on a single network via the switches. Both methods are applied in Figure B-1. In addition, backup ISPs for each location have been added, as well as a new firewall for the Memphis branch. There is still also a question of whether the overall offices should be linked by anything else other than the ISPs’ connections to the Internet. Any hardware category and role that are present in both offices is labelled with a prefix with the city name to reduce ambiguity as to which phone/WAP/etc goes in which office.

**Figure B-1**

Tentative Network Diagram for SNHUEnergy, Inc. (Dallas and Memphis branches)



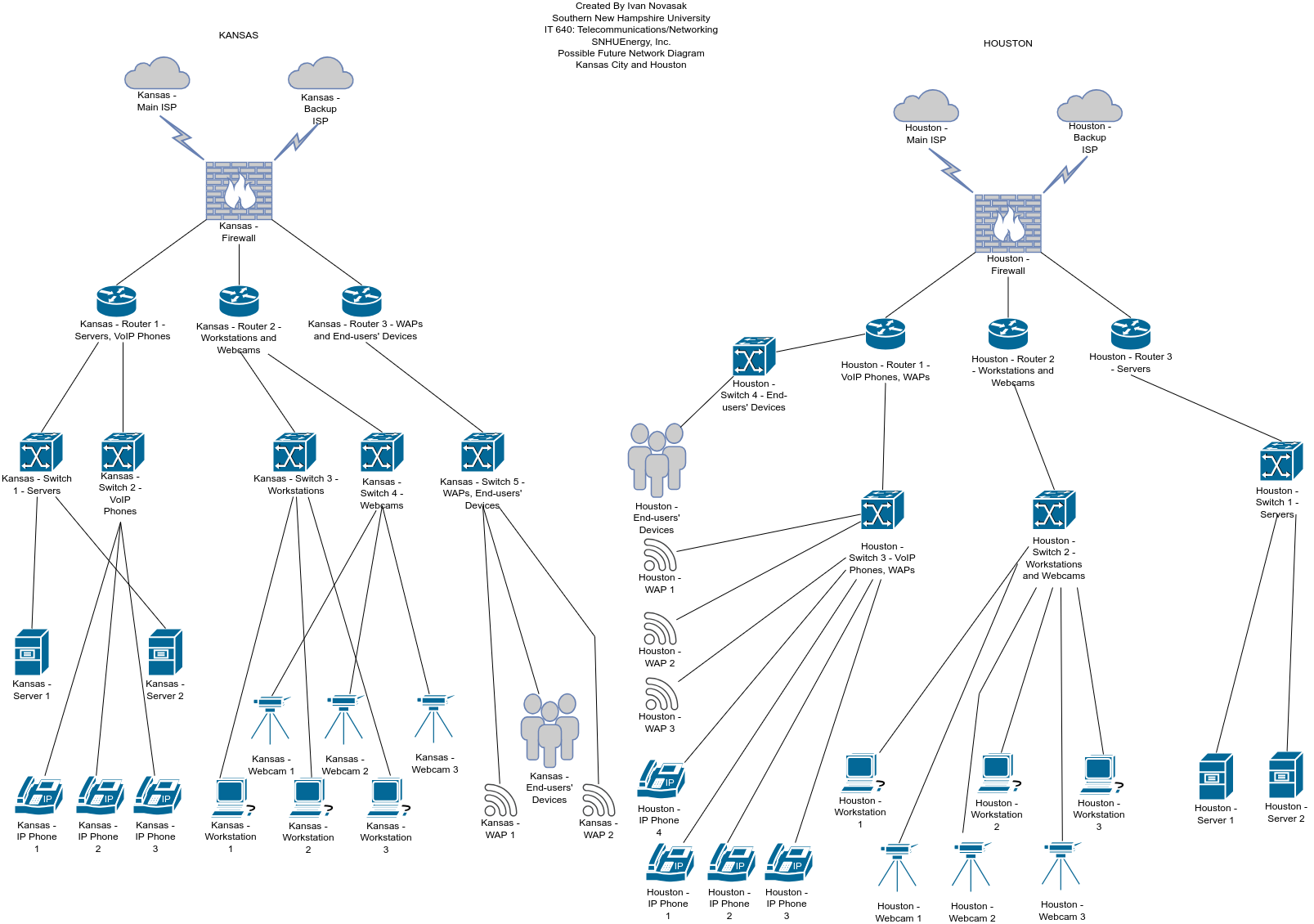
*Note*: Adapted from Hughes (2024a/b/c) and Novasak (2024b).

***Kansas City and Houston***

Figure B-2, shown below, shows a possible arrangement for Kansas City and Houston’s branch office networks.

**Figure B-2**

Tentative Network Diagram for SNHUEnergy, Inc. (Kansas City and Houston branches)



*Note*: Adapted from Hughes (2024a/b/c) and Novasak (2024b).

**Planning and Security**

The next section of this document concerns planning for implementation and enforcing security on the new network via management tools and security devices, as well as the risks of not implementing the network upgrades.

**Mitigating Performance and Security Issues**

***Performance***

The performance issues to be addressed include router overload, bandwidth, and wireless coverage. Wireless coverage can be extended by adding more access points around the office (Sharma, 2022). Having routers in general can allow increased bandwidth transmission by sharing the load across multiple routers instead of having an entire office’s network traffic going through just 1 router (Sharma, 2022). Jomilė Nakutavičiūtė, of NordVPN, recommends upgrading ISPs to one that offers higher bandwidth, using a VPN to avoid any throttling the ISP may be doing, and limiting the devices connected via WiFi to only those that specifically require WiFi and can not be wired (Nakutavičiūtė, 2022).

***Security***

The first security vulnerability to address involves unauthorised connections that send dangerous data like viruses or malware into the company. Having a firewall for the network as well as antivirus/antimalware software on the computers at the offices will work against threats from the outside world (Barney & Lutkevich, 2022).

To keep buildings and any other physical devices secure from access by unauthorised users, multifactor authentication (MFA), which is a form of authentication that requires the user to have a physical object on their person as well as enter a password or passcode for entry, will be employed. This should be in addition to more traditional forms of building security like guards, cameras, security alarms that also contact law enforcement when breaches happen.

Linda Rosencrance and Madelyn Bacon, of TechTarget, point out another avenue of attack from malicious people known as social engineering (Rosencrance & Bacon, 2021). This involves an attacker trying to get information about how the company’s internal functions, sometimes starting with employees with lower level access before moving onto people who have higher levels of access (Rosencrance & Bacon, 2021). They try to probe people for information that can be useful in the attack (Rosencrance & Bacon, 2021). Also, dumpster diving and fraudulent email links are considered social engineering as they rely on human error for the attack to get confidential information or unauthorised access (Rosencrance & Bacon, 2021). To prevent social engineering from getting around the firewall and MFA, there needs to be a clear policy on social engineering and have all employees be aware to never give passwords or any sensitive information out over the phone or other communications media. This includes never giving such information to trusted parties, in case a security breach does happen. In this policy there should also be guidelines on who to report to if one thinks a breach has happened, as well as rules on not discussing confidential matters outside the protected zone where such discussion is done. Email social engineering can be dealt with via a scanning system for emails that checks for suspicious content or links (Rosencrance & Bacon, 2021). Cloud 7 IT Services has a comprehensive cybersecurity awareness educational programme that teaches about phishing , strong password practice, simulation of real-world scenarios, and the ability to customise the training programme to the needs of SNHUEnergy, Inc. (Cloud 7, n.d.).

Having a reliable Internet connection is essential to having a business that is secure. The big change to take place is having each office have their own dedicated Internet connections: a primary and a secondary connection. That way the office and its network will be able to continue functioning should there be a problem with one of the ISPs.

**Beneficial Network Management Software**

***AKIPS***

AKIPS network monitoring software is a comprehensive monitoring suite that does visibility/discovery of all devices on the network, alerting, event handling, reporting, and integration with third-party apps like ‘Microsoft Teams, Opsgenie, PagerDuty, ServiceNow, Slack and Splunk’ (Smoliak, 2024). Discovery with AKIPS works by pinging the IP addresses on the network which is less overwhelming to the network than ‘pulling back ARP, routing or bridging tables’ (Smoliak, 2024). The discovery is so quick and efficient that it can discover 5000 switches and routers in just 10 minutes (Smoliak, 2024). AKIPS has intelligent polling that monitors interface state every 60 seconds, reducing SNMP traffic by 60% and doesn’t require an SQL database (Smoliak, 2024). This tool also has statistics tracking via NetFlow and syslog tracking which tracks which devices are communicating with each other (Smoliak, 2024).

AKIPS provides a powerful alerting system with customisable alerts based on the type of alerting the network administrator is looking for, a GUI system that shows 60-second intervals over the previous 3 years (rolling), and an events dashboard showing the most important network events in one place (Smoliak, 2024). This software can also show unused devices over the last 365 days with a breakdown by device and interface name, interface state and state change, and VLAN (Smoliak, 2024). Videos that show how to use and deploy AKIPS are located at <<https://www.akips.com/videos/>>. AKIPS is paid for by annual subscription, and a quote can be obtained at <<https://www.akips.com/get-a-quote/>> (AKIPS, 2024).

**Security Devices**

The devices on this network that will ensure better security than on the existing network include extra routers, firewalls that separate each office network from the ISPs’ Internet links, and having antivirus/anti-malware software on all PCs connected to the network. Using these in conjunction with a VPN and AKIPS will enhance the already existing security provided by the hardware.

***Routers***

Routers segregate devices into separate networks. According to SureLock Technology, this ensures the sensitive data traffic going to and from the servers will not flow into consumer devices or general employee devices at the company and allows for balancing traffic loads based on the type of devices (still depending on how many devices are connected and available bandwidth) (SureLock Technology, n.d.). Segmented networks allow for easier-to-manage networks and more control over different areas of the network (Barney & Lutkevich, 2022). This allows for instance the ability to prioritise VoIP calls which require real-time communication over emails which are an asymmetric form of communication and therefore have a more acceptable delay allowance.

***Firewalls***

The firewalls are being used to inspect and allow only authorised traffic through into or out of the network (Barney & Lutkevich, 2022). They can block ‘application-layer attacks and provide advanced malware defense with inline deep packet inspection’ and are a form of intrusion protection system (IPS) (Barney & Lutkevich, 2022). Firewalls can also be configured so that employees can not access sites that are dangerous to the network or not conducive to productivity, such as pornography or file sharing sites (Barney & Lutkevich, 2022).

***Multifactor Authentication***

Multifactor Authentication (MFA), detailed by Kinsa Yasar and Mary E. Shacklett of TechTarget, while not a device itself, is a security technique that typically involves the user knowing some secret password or passphrase, having a particular device like a smartphone or key fob, and/or using their fingerprint or facial scan to authenticate themselves (Yasar & Shacklett, 2023). SNHUEnergy can use this for employees accessing the buildings as well as logging into the computers. Ideally, the user’s phone would be registered to the MFA system so that after they arrive onsite or turn the computer on then enter their password, they are then asked for a one-time-password that was sent to their phone’s authentication app (such as Google Authenticator) that they’ll need to provide to access the building or computer system (Yasar & Shacklett, 2023).

***Virtual Private Network***

According to Alexander S. Gillis, of TechTarget, a Virtual Private Network (VPN) is a scheme where network traffic is encrypted in a network tunnel before it is sent over insecure public networks like the Internet (Gillis, 2021). It is essential for any employees to use a VPN when accessing SNHUEnergy’s network from outside the company, like when working remotely (Gillis, 2021). Gillis states that connection speeds can be a bit slower when using a VPN, so SNHUEnergy may need to invest in a higher bandwidth connection if the speeds they experience when using the VPN aren’t sufficiently fast enough (Gillis, 2021).

**Changes for Existing Devices on the Network**

Most of the changes being made involve adding more of the same type of devices into the network, as opposed to new types of devices entirely. For instance, the Dallas office originally had 1 firewall, 1 router, and 2 switches and after the upgrades, will have 1 firewall, 3 routers, and 6 switches. Similarly, the Memphis office had no firewall, 1 router, and 1 switch before, which will be upgraded to have 1 firewall, 3 routers, and 6 switches. In addition, the Dallas network had only 1 Internet connection before and the Memphis network had no dedicated Internet connection and just ran off the Dallas connection. After the upgrade, each office will have their own dedicated Internet connections: 1 primary and a second as a backup in case the main 1 has issues. The diagrams in Figures A-1, B-1, and B-2 show the differences graphically between the original network and proposed new networks.

**Challenges of Implementing This New Network**

The biggest challenge to implementing the new network is likely to be costs for both the hardware as well as possibly training new staff on running this larger 4-site network.

The hardware for the additional components has the following average costs, according to Livewire, LCC (2022):

* RJ45 Jacks: $10 - $25 each;
* WiFi Extenders: $30 - $100 each;
* Cable management strips: $35 - $95 each;
* Cable runners: $20 - $30 each;
* Ethernet cabling: $0.25 - $0.75 per foot (about $0.80 to $2.50 per metre);
* Fibre-optic cabling: $1 - $6 per foot ($3.30 to $20 per metre);
* Modems and routers: $200 - $500 on average for each, with high-end models $1500 and more.

Labour costs of a network upgrade are another significant factor to consider. Livewire (2022) estimates that these costs range from $50 - $250 per hour and a rough estimate of needing 30 - 40 hours of work for every 2,000 feet (609.6 metres) of cable per office.

Anish Devasia, of The Network Installers out of California, presents some estimates in the range of $1,000 for the most basic of office networks to over $10,000 for more complex networks, where these costs include ‘hardware, cabling, and installation services’ (Devasia, 2024).

**Risks to SNHUEnergy, Inc. of Not Making These Changes**

## According to Doug Coleman, the chief operating officer of Roebuck Technologies, not adhering to good cybersecurity principles can lead to data loss, cyberattacks that slow or stop productivity altogether, government fines for violations of regulations like General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability Act of 1996 (HIPAA), ransomware extortion with the possibility of still losing data to hackers, a bad public reputation, and class-action lawsuits centred on the victims of cybercrime that was allowed by the company (Coleman, 2021).

According to Rocket IT’s article entitled *Should Your Company Invest in a Secondary (Backup) ISP?*, not having a backup ISP can cost SNHUEnergy ‘thousands of dollars in lost productivity’ should there be a problem with the ISP SNHUEnergy is using (Rocket IT, 2016). Having a second ISP allows both the ability to keep running should one ISP lose connectivity, as well as the ability to simultaneously utilise both ISPs for more bandwidth depending on which devices are heavier users of bandwidth at the time (Rocket IT, 2016). This latter point is known as load-balancing (Rocket IT, 2016).

# References

AKIPS. (2024, March 5). *Get a quote*. AKIPS. <https://www.akips.com/get-a-quote/>

Barney, N., & Lutkevich, B. (2022, October 5). *network security*. TechTarget. <https://www.techtarget.com/searchnetworking/definition/network-security>

BasuMallick, C. (2022, July 29). *RTP Meaning, working and uses*. Spiceworks, Inc. <https://www.spiceworks.com/tech/networking/articles/what-is-rtp/>

Chai, W. (2021, May 3). *VoIP phone*. TechTarget. <https://www.techtarget.com/searchunifiedcommunications/definition/VoIP-phone>

Chai, W., & Lazar, I. (2021, August 23). *video conferencing*. TechTarget. <https://www.techtarget.com/searchunifiedcommunications/definition/video-conference>

Chip. (2023, December 5). *What are the components of a relational database?* QuantHub. <https://www.quanthub.com/what-are-the-components-of-a-relational-database/>

Cloudflare. (n.d. a). *What is a network switch? | Switch vs. router*. Cloudflare, Inc. <https://www.cloudflare.com/en-gb/learning/network-layer/what-is-a-network-switch/>

Cloudflare. (n.d. b). *What is SSH? | Secure Shell (SSH) protocol*. Cloudflare, Inc. <https://www.cloudflare.com/en-gb/learning/access-management/what-is-ssh/>

Cloud 7. (n.d.). *Cybersecurity Awareness training*. Cloud 7 IT Services Inc. <https://cloud7itservices.ca/cybersecurity-awareness-training>

Coleman, D. (2021, May 6). *Consequences of poor cybersecurity management and how to avoid becoming a statistic*. Roebuck Technologies. <https://www.roebucktech.com/it-blog/consequences-of-poor-cybersecurity-management-and-how-to-avoid-becoming-a-statistic/>

Darah, D. (2022, April 18). *7 types of networks and their use cases*. TechTarget. <https://www.techtarget.com/searchnetworking/feature/7-types-of-networks-and-their-use-cases>

Devasia, A. (2024, February 3). *Small business network setup cost: Pricing guide for 2024*. The Network Installers. <https://thenetworkinstallers.com/blog/small-business-network-setup-cost/>

English, J. (2022, April 14). *An introduction to 8 types of network devices*. TechTarget. <https://www.techtarget.com/searchnetworking/tip/An-introduction-to-8-types-of-network-devices>

Fortinet. (n.d.). *What does a firewall do?*. Fortinet. <https://www.fortinet.com/resources/cyberglossary/what-does-a-firewall-do>

GeeksforGeeks. (2022, March 21). *Devices used in each layer of TCP IP model*. GeeksforGeeks. <https://www.geeksforgeeks.org/devices-used-in-each-layer-of-tcp-ip-model/>

Gillis, A. S. (2021, September 17). *VPN (virtual private network)*. TechTarget. <https://www.techtarget.com/searchnetworking/definition/virtual-private-network>

Hughes, C. (2024a). *SNHUEnergy Inc. - Organizational Network Diagram - Physical Network Design*. Southern New Hampshire University. <https://learn.snhu.edu/content/enforced/1504959-IT-640-Q3549-OL-TRAD-GR.24TW3/Course%20Documents/IT%20640%20Organizational%20Network%20Diagram%20Current.pdf?isCourseFile=true&ou=1504959>

Hughes, C. (2024b). *SNHUEnergy Inc. - Dallas Office Network Diagram - Logical Network Design*. Southern New Hampshire University. <https://learn.snhu.edu/content/enforced/1504959-IT-640-Q3549-OL-TRAD-GR.24TW3/Course%20Documents/IT%20640%20Dallas%20Office%20Network%20Diagram%20Current.pdf?isCourseFile=true&ou=1504959>

Hughes, C. (2024c). *SNHUEnergy Inc. - Memphis Office Network Diagram - Logical Network Design*. Southern New Hampshire University. <https://learn.snhu.edu/content/enforced/1504959-IT-640-Q3549-OL-TRAD-GR.24TW3/Course%20Documents/IT%20640%20Memphis%20Office%20Network%20Diagram%20Current.pdf?isCourseFile=true&ou=1504959>

Hughes, C. (2024d). *Milestone One Guidelines and Rubric - IT-640-Q3549 Telecommunications/Networking 24TW3*. Southern New Hampshire University. <https://learn.snhu.edu/d2l/le/content/1504959/viewContent/29855161/View>

Hughes, C. (2024e). *IT 640 Final Project Scenario*. Southern New Hampshire University. <https://snhu-media.snhu.edu/files/course_repository/graduate/it/it640/it640_final_project_scenario.pdf>

John, G. (2023, October 31). *What is network interface card (NIC)?* Tutorials Point. <https://www.tutorialspoint.com/what-is-network-interface-card-nic>

Kelly, W. (2022, December 14). *wireless access point*. TechTarget. <https://www.techtarget.com/searchmobilecomputing/definition/access-point>

Livewire. (2022, October 23). *How much should my office network cost?* Livewire, LLC. <https://www.getlivewire.com/office-network-cost/>

Loshin, P., & Cobb, M. (2021, September 24). *Secure Shell (SSH)*. TechTarget. <https://www.techtarget.com/searchsecurity/definition/Secure-Shell>

Nakutavičiūtė, J. (2022, April 7). *How to Increase Internet Speed [Tips]*. NordVPN. <https://nordvpn.com/blog/increase-wifi-bandwidth/>

Novasak, I. (2024a, March 17). *SNHUEnergy, Inc: Project Analysis Plan*. Southern New Hampshire University.

Novasak, I. (2024b, March 31). *SNHUEnergy, Inc: Current Network Architecture*. Southern New Hampshire University.

Posey, B. (2021, August 18). *What is a Server?* TechTarget. <https://www.techtarget.com/whatis/definition/server>

QuoStar. (2019, October 14). *Why your business needs two Internet connections*. QuoStar Solutions Limited. <https://www.quostar.com/blog/why-your-business-needs-two-internet-connections/>

Ravikiran, A.S. (2023, May 22). *Differentiating SQL and MySQL: A Comprehensive guide*. Simplilearn Americas Inc. <https://www.simplilearn.com/tutorials/sql-tutorial/difference-between-sql-and-mysql>

Rocket IT. (2016, January 28). *Why your company should invest in Backup ISP*. Rocket IT. <https://rocketit.com/backup-isp/>

Rosencrance, L., & Bacon, M. (2021, June 3). *social engineering*. TechTarget. <https://www.techtarget.com/searchsecurity/definition/social-engineering>

Rural Telecommunications of America (RTA). (n.d.). *Benefits of having multiple web connections for businesses*. Rural Telecommunications of America, Inc. <https://rtatel.com/the-benefits-of-having-multiple-internet-connections-for-businesses/>

Shahid, S. (2022, September 29). *which devices are used with respect to each layer of the OSI model?* Medium. <https://medium.com/@_salmanshahid/which-devices-are-used-with-respect-to-each-layer-of-the-osi-model-ce11788480ff>

Sharma, D. (2022, September 12). *Should You Use More Than One Router? The Pros and Cons.* MakeUseOf (MUO). <https://www.makeuseof.com/should-you-use-multiple-routers-pros-and-cons/>

Shaw, K. (2024, January 23). *The OSI model explained and how to easily remember its 7 layers*. Network World. <https://www.networkworld.com/article/964816/the-osi-model-explained-and-how-to-easily-remember-its-7-layers.html>

SureLock Technology. (n.d.). *Does having two routers slow down internet*? Kopesky Enterprises Inc. <https://surelocktechnology.com/blog/does-having-two-routers-slow-down-internet>

Shyam, P. (2019, August 1). *How to know if two IP addresses are in the same network*. LinkedIn. <https://www.linkedin.com/pulse/how-know-two-ip-addresses-same-network-priyanka-kumari/>

Simic, S. (2023, September 5). *What is 127.0.0.1 Localhost?* phoenixNAP. <https://phoenixnap.com/kb/127-0-0-1-localhost>

Smoliak, H. (2024, April 15). *Features*. AKIPS. <https://www.akips.com/features/>

Snom. (n.d.). *G.711*. Snom Technology Gmbh. <https://service.snom.com/display/wiki/G.711>

TechTarget Contributor. (2023, December 8). *network interface card (NIC)*. TechTarget. <https://www.techtarget.com/searchnetworking/definition/network-interface-card>

uCertify. (n.d.). *Lesson 2 : Network Topologies and Types -UCertify*. uCertify. <https://www.ucertify.com/app/?func=ebook&chapter_no=3#076jS>

Villanueva, M.S. (2021, October 12). *3 Top Risks of Not Having a Firewall*. Intelligent Technical Solutions. <https://www.itsasap.com/blog/3-top-risks-of-not-having-a-firewall>

Yasar, K., & Shacklett, M. E. (2023, October 2). *multifactor authentication*. TechTarget. <https://www.techtarget.com/searchsecurity/definition/multifactor-authentication-MFA>

Yasar, K., & Lutkevich, B. (2023a, April 19). *firewall*. TechTarget. <https://www.techtarget.com/searchsecurity/definition/firewall>

Yasar, K., & Lutkevich, B. (2023b, December 11). *Transmission Control Protocol (TCP)*. TechTarget. <https://www.techtarget.com/searchnetworking/definition/TCP>