James Osibogun

9-1 Final Project Submission: Network Analysis and Architecture Evaluation

SNHU

Professor Mobley

**Executive Summary**

The Memphis and Dallas networks need to readjust to accommodate two more networks. Dallas and Memphis are currently sharing a network with a cloud security system. They must implement TCP/IP addresses and decide the topology for all four networks. The networks will include routers, switches, computers, VIoP, Conference cameras, and servers.

There are ways to approach implementing a new network. The lifecycle approach to network design plans, prepares, implements, operates, and optimizes **(PPDIOO). PPDIOO** lowers the cost of network ownership, increases network availability, and applies quick access to applications and services. Network planning can take place on a whiteboard where the network planner shares ideas with their team or a multi-departmental change control meeting to discuss 3-layer management.

The overall risk of organizations is security. The new network PPDIOOs prepare methodology to plan security by recommending the best approach to mitigate performance and security issues and challenges. The result is to calculate the subnets and hosts. The network engineer is to leave no ports open for hackers and implement Wireshark.

**Physical Network Devices**

Physical Network Devices have network routers, switches, and security system equipment. It utilizes data, voice, and video applications across the organization (SNHU).

The offices have Viop, Servers, Routers, switches, and end users.

**Critical Traffic Patterns**

The packet list pane displays all the packets in the current network. In the capture, we have the source, the package address from source 67.16.104.172, with a destination of 10.0.6.73. The protocol is RTP, with a length of 216.

Patterns Across the Infrastructure in the packet bytes show a hex dump of the packet data. Each of the lines causes a data offset. We can follow the capture using Wireshark of Line/ T-shark.

Wireshark captures packets from a network connection, such as from your computer to your home office or the internet. The package is the name given to a discrete data unit in a typical Ethernet network.

In Wireshark, the specialist can look at the hex decimal and pinpoint address resolution protocols by looking at the hardware type, protocol type, hardware size, protocol size, opcode request, sender Mac address, target MAC (Media Access Control), target IP address, and sender IP address.

Network Engineers must use Wireshark to locate unused ports. The purpose of finding new ports is to prevent hackers from using the port and navigating through the network unnoticed. In Wireshark, the network Engineer (NE) can pinpoint users' location in the network. For example, in Wireshark, the NE can identify the building number, the room that is using the network.

**Performance Issues**

To look at the protocols, we can filter protocols by looking at or searching RTP (Real transport protocol). We can also filter out source 67.16.104.172, and it will display all the RTPs.

Layer Two networks forward all traffic. When the broadcast traffic creates congestion and decreases network efficiency, congestion on a network can be challenging to minimize a problem and find a solution.

An enterprise WAN (Wide Area Network) is often built for one organization and is usually private. Often, enterprise WANs (Wide Area Network) are created using leased lines involving a direct point-to-point connection between two personal sites. Given their capability and use, WANs have several benefits, including centralizing IT infrastructure (SNHU (Southern New Hampshire University)).

Layer Three restricts broadcast traffic to the local network by reducing overall traffic levels. It allows administrators to divide networks into smaller parts and restrict broadcasts (SNHU). Layer Three is responsible for the capability that business networks require the most—routing controls. Despite WANs' ability to boost privacy, they open the way for certain types of internal security breaches, such as unauthorized use, information theft, and malicious damage to files.

**Security Issues**

Security issues must isolate source ports and destination ports. Using Wireshark, we can determine and acknowledge the port we want and the port we do not wish to use by using the port number. Another security issue is DDoS attacks.

RST hijacking involves injecting an authentic-looking reset (RST) packet using a spoofed source address and predicting the acknowledgment number. The hacker can reset the victim's connection if it uses an accurate acknowledgment number (Gitbooks, n.d).

**Challenges in Network Security include:**

* misconfiguration proliferation,
* Lax control of privileged access,
* Tool interoperability shortcomings,
* Lack of visibility, and
* Commands that are out of step with infrastructure changes.

Network solutions should be comprehensive, automating network security in every aspect, from policy design to implementation. It should support real-time monitoring of live data for updated information streaming. Subnets should scale in all directions, collecting security details and normalizing device rules for storage in a unified database.

**Current Network Architecture**

Network Architecture comprises network routers, switches, and security system equipment. Networks connect all the users to the internet. All the connectivity between the users is Transmission Control Protocol/Internet Protocol (TCP/IP) traffic. Utilization is captured by data, voice, and video applications across the organization (SNHU).

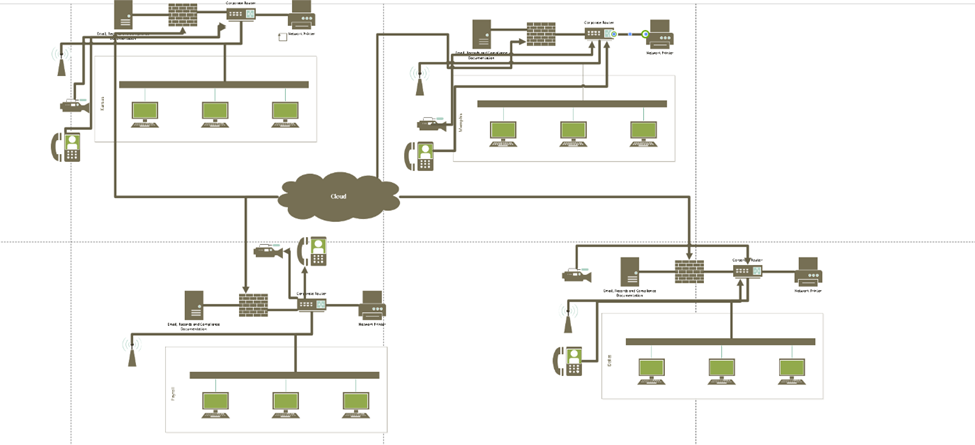
**Future Network Architecture**

The needs of this network setup are equipment and internet connectivity and connecting computers, router configuration. The equipment needed is computers, a surge strip, a router, and cables. The router configuration needs a change to the default password, create ssid, activate wireless encryption and activate DHCP. The plan for the network requires a centralized router that supports wired and wireless connections (Oja). The router IP address might be 192.168.1.1 or 192.168.1.100. Ensure the router has sufficient ports for Ethernet; have 802.11a, b,g, and 802.11n. Before using a network adjustment to the router configuration, ensure the network is secure. Using the computer browser to access the router configuration is an alternative. The new networks must consider options like wireless encryption. The protocol is called WEP (Wired Equivalent Privacy).

A network architecture that would be appropriate for supporting the ultimate growth of the organization and defending how this recommended network would improve communication across the company is to have a network to allow the Houston and Kansas networks to communicate with their servers and routers.

Expanding the network, SNHU Energy must allow the file-sharing of specific files and public folders. However, file sharing has security risks because they are subject to misuse and modifications, which can be hacker prone. To combat hackers to a file, implement permission to files, limit sharing to specific people, and remove sharing from files you no longer want to share.

Mesh topology creates sufficient redundancy without the complexity of a full mesh. A partial mesh topology is used for larger installations. Each device is connected to at least two other devices in a partial mesh topology.



**Planning and Security**

During the Planning and Security, A new network must not have the same default password. Network devices include wireless access points. This point must be pre-configured with default administrator passwords to simplify setup. These default passwords are readily available online and provide only marginal protection. If the user were to change their default passwords, it would make it harder for attackers to access the device (CISA, 2021) and steal potential information crucial to the organization.

You can restrict access to your network by filtering these MAC addresses (CISA, 2021). ensuring fewer people are on the server. Only allow certain people to access the network.

Encryption prevents anyone from accessing your network and viewing it. Wi-Fi Protected Access (WPA), WPA2, and WPA3 encrypt information transmitted between wireless routers and devices (CISA, 2021).

Wi-Fi routers allow users to protect their device's SSID (Service Set Identifier). Protect your Service Set Identifier (SSID) from outsiders. Avoid publicizing your SSID. Install antivirus software to keep your virus definitions current (CISA, 2021). The software and virus protection must be present. If the network is protected, hackers will have more difficulty sending viruses and malware. Your wireless access point manufacturer will periodically release updates to and patches for a device's software and firmware (CISA, 2021).

**Network management tool**

SNHU Energy needs a network management tool to expand its network. According to Kaseya, [VSA](https://www.kaseya.com/products/vsa/) provides [SNMP device monitoring. We](https://www.kaseya.com/products/vsa/network-monitoring/) have "zero configuration" standard SNMP monitoring, which means you have only one thing to do to enable this function" (Kaseya, 2022).

Cloud-based network management allows businesses to manage their networks remotely. It is essential to implement management for the network must be accessed via a web browser or desktop client. The distinct types of network management are Fault management, Configuration management, accounting management, Performance management, and Security management (CISA, 2021).

**Types of security devices**

SNHU Energy must have specific security devices Like Firewalls. They are one of the most fundamental network security appliances. Firewalls can come in hardware or software forms.

**Intrusion Protection Systems (IPS)**

Network-based intrusion protection systems proactively monitor all traffic. The SNHU Energy network has pre-made profiles, signature detection, artificial intelligence, and anomaly detection. IPS systems can detect many network intrusions, from malware on endpoint devices to denial-of-service attacks (Restorepoint, n.d).

**Unified Threat Management (UTM)**

UTMs (Unified Threat Management) combine SNHU Energy network firewalls. It has an intrusion detection system, an intrusion prevention system, and other features.

Network Access Control

Endpoint devices for the corporate network are critical to security. As a result, network access requires authentication. (Restorepoint,n.d).

**Email Security Gateways**

Email Security Gateways monitors incoming and outgoing email traffic. Recently, advances in email security found that gateways use historical data and statistical analysis to detect anomalies more accurately (Restorepoint,n.d) for spam, viruses, phishing attempts, and compromised accounts.

**VPN Gateways &** **Network Device Backup and Recovery**

SNHU must have a virtual private network. Traffic enters the internal network. The onsite technician performs a site survey to document the network structure. It is also necessary to investigate and report on the physical layout of the premises (Pearson highered,n.d).

A site survey can give the network designer valuable information and create an appropriate starting point for the project. It shows what is on site and what is needed (Pearson Highered,n.d). This information is gathered from different people.

**Site Survey Information**

To determine the number of network users the network must support, consider how many users will be added over the next 12 months and how many network printers and network servers the web must accommodate.

A network is a long-term investment. Planning for future growth can save a great deal of time, money, and frustration. It is essential to identify the needs of applications, especially voice and video. These applications may require additional network device configuration and new ISP services to support the necessary quality. Documenting designs that load on the current devices is also required. New services required Will be implementing VoIP or videoconferencing technology. Security and privacy currently have a security system to protect the network. Although this connectivity offers exciting opportunities for information sharing, it also threatens information not meant for sharing. Each wireless access point connecting the wireless desktop and wireless laptop computers to the web has a range. It is possible to connect computers, printers, and other devices to the network using a traditional wired network (10/100 switched Ethernet), a wireless-only network (802.11x), or a combination of wired and wireless networking. To estimate the required access points, knowledge of the area of coverage needed and the physical characteristics of the location the wireless network must cover. The project budget usually decides what can and cannot be done using Cost-benefit analysis alone.

**Planning and Security**

Network management tools used Logic Monitor Performance Monitor can be used to monitor the network. Logic Monitor allows you to discover and map relationships between critical infrastructure resources and their dependencies, enabling you to find and map relationships between essential infrastructure resources and their dependencies. Anomaly detection and forecasting capabilities elevate network performance visibility and help prevent downtime by identifying future bandwidth issues and performance bottlenecks.

We can encrypt devices with McAfee and give training on all devices, which are company devices that shall be imaged with customized images allowed to connect to the company domain for easy use. But the machines must be authenticated by users using two-factor authentication, which might be expensive but can save the company more money in the long run.

**Recommendations**

Recommendations are Infrastructure-as-a-Service, commonly called "IaaS," a form of [cloud computing](https://www.ibm.com/in-en/topics/cloud-computing) that delivers fundamental computer, network, and storage resources to consumers on-demand, over the internet, and on a pay-as-you-go basis. Infrastructure-as-a-Service, commonly called "IaaS," is a form of [cloud computing](https://www.ibm.com/in-en/topics/cloud-computing) that delivers fundamental compute, network, and storage resources to consumers on-demand, over the internet, and on a pay-as-you-go basis.

Compared to traditional IT, **IaaS** gives customers more flexibility, builds out computing resources as needed, and scales them up or down in response to spikes or slowdowns in traffic. IaaS use cases are Ecommerce, Disaster recovery, Internet of Things (IoT), and event processing. Deploying standalone email encryption services can be so cumbersome to manage and use that many users bypass their organization's secure communication policies. **Barracuda** provides simple **email encryption** that is highly secure and part of a complete email protection solution. More critical, Barracuda combines email encryption with other layers of data protection, including data-leak prevention, archiving, and filtering, that block malware and advanced threats.

**Conclusion**

In conclusion, for this business to grow, it would need more equipment like servers. They could add a marketing department and a finance department. Based on the conceptual design, the added server, switches, and routers must be included in the growth of the program's database**.**

Network's logical and physical design, including planning and components of a rational network design, the physical network, and planning resources.

A subnet, or subnetwork, is a [network](https://www.cloudflare.com/learning/network-layer/what-is-the-network-layer/) inside a network. Subnets make networks more efficient. Network traffic can travel a shorter distance through subnetting without passing through unnecessary [routers](https://www.cloudflare.com/learning/network-layer/what-is-routing/) to reach its destination (Cloudflare,n.d). Also, RAID and UPS help with load balancing to protect the network.

The network will be described by different classes, which must be classed A through E. Since Dallas is significant, it must be able to connect a bunch of devices. Memphis and the two new networks will, in turn, add more servers.

VLSM subnetting, which is classless. CIDR (Classless inter-domain routing) Classless shows that we abandon classes A, B, and C.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Subnet** | 1 | 2 | 4 | 8 | 16 | 32 | 64 | 128 | 256 |
| **host** | 256 | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
| **Subnet**  **mask** | /24 | /25 | /26 | /27 | /28 | /29 | /30 | /31 | /32 |

Since the company is banking on more than 120 host. To surpass 50 percent. The subnet mask will be /24 with host of 256.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Subnet** | 1 | **2** | 4 | 8 | 16 | 32 | 64 | 128 | 256 |
| **host** | 256 | **128** | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
| **Subnet**  **mask** | /24 | **/25** | /26 | /27 | /28 | /29 | /30 | /31 | /32 |

Given range:

|  |  |  |  |
| --- | --- | --- | --- |
| **Network ID** | **Subnet mask** | **Host** | **Network** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

In the end we must determine how many hosts per Network ID, subnet mask, host, and network. We must add rows based on subtracting or dividing host based on how big or small the subnet and the host. SNHU must set up a TCO budget before proceeding with this project. There must be a logical plan and a physical plan. The network administrator and the stakeholder of SNHU Energy must sign off on these plans. My final analysis is to have all names of users and locations. A list of who requires data sharing, training on how to make strong passwords, and does not use generic passwords. Based on the Wireshark image, users should not leave any ports unused.

**Reference:**

Cisco (November 18, 2020). Network Address Translation (NAT). Retrieved on February 18, 2023 from <https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html>

[Rogers, B(n.d). Legal and Ethical Considerations for Digital Forensics. Retrieved on February 18, 2023 from https://www.pluralsight.com/courses/legal-ethical-considerations-digital-forensics](https://usc-word-edit.officeapps.live.com/we/Rogers,%20B(n.d).%20Legal%20and%20Ethical%20Considerations%20for%20Digital%20Forensics.%20Retrieved%20on%20February%2018,%202023%20from%20https:/www.pluralsight.com/courses/legal-ethical-considerations-digital-forensics)

# Testking(n.d). Identify typical applications and their impact on the network. Retrieved on February 18, 2023 from <https://www.test-king.com/guide-identify-common-applications-and-their-impact-on-the-network.htm>

Drager,N(April 9, 2020). **Single Router vs. Multi-Point Access:** Which is Better for Your Business? Retrieved on February 18, 2023, from <https://quantumpc.com/single-router-vs-multi-point/#:~:text=Some%20of%20the%20key%20issues,extending%20your%20Wi%2DFi%20signal>

Softwaretestinghelp(n.d).7 Layers Of The OSI Model (A Complete Guide). Retrieved on February 18, 2023, from <https://www.softwaretestinghelp.com/osi-model-layers/>

# 

Kaspersky(n.d). What is a firewall? Definition and explanation.Retrieved on February 18, 2023, from <https://www.kaspersky.com/resource-center/definitions/firewall>

Netgear(n.d). What-is-a-switch-An-introduction. Retrieved on February 18, 2023, from <https://kb.netgear.com/232/What-is-a-switch-An-introduction>

CCNA blog (n.d). Static routing.Retrieved on March 5, 2023, from <https://www.ccnablog.com/static-routing/>

KTflash (n.d) Network Level Session Hijacking. Retrieved on March 5, 2023, from <https://ktflash.gitbooks.io/ceh_v9/content/103_network_level_session_hijacking.html>

Informit(November 13, 2003) Network Design Strategies. Retrieved on March 5, 2023 from

<https://www.informit.com/articles/article.aspx?p=101762>

Cloudflare(n.d).What is a subnet? | How subnetting works Retrieved on March 5, 2023, from

<https://www.cloudflare.com/learning/network-layer/what-is-a-subnet/>