Gentian Hoxha

05/23/2025  
IT-640 Telecommunications and Networking  
SNHU Energy Final Network Architecture Project  
[**gentian.hoxha@snhu.edu**](mailto:gentian.hoxha@snhu.edu)

**Executive Summary**

This report provides a complete analysis of the current and future network architecture for SNHUEnergy, which operates across Dallas and Memphis offices. Key findings include a lack of redundancy, a heavy reliance on the headquarters for critical applications like SQL databases and VoIP, and security risks due to weak VPN encryption and missing firewalls. An updated architecture featuring SD-WAN, cloud integration, zero-trust security, and updated network monitoring tools is recommended. Diagrams illustrate current and future traffic flows and device placements. These changes aim to boost network reliability, security, and scalability.

**Current Network Architecture**

**Network Applications**

Considering SNHUEnergy, operates across two locations like Dallas and Memphis. Each office supports key parts of the business. The Dallas office handles critical functions like email, payroll, accounting, and HR, while the Memphis office is focused on billing and operations. Both locations also use VoIP phone systems and video conferencing to stay connected internally and externally.

**OSI Model**

The current network setup aligns with the OSI model in the following ways:

* **Layer 1 – Physical**: Includes all the cables and wireless access points that keep the devices connected.
* **Layer 2 – Data Link**: The switches at each location direct internal network traffic within the office.
* **Layer 3 – Network**: The routers help move data between offices and to the internet.
* **Layer 4 – Transport**: This layer ensures services like VoIP and video calls run smoothly.
* **Layer 5 – Session**: Manages the sessions for those calls and conferencing systems.
* **Layer 6 – Presentation**: Takes care of data formatting and encryption especially important for secure communication.
* **Layer 7 – Application**: Where end user tools like email, billing systems, and HR platforms live.

**Key Network Components**

* **Routers** connect the offices to each other and to the internet.
* **Switches** are responsible for linking up devices like workstations, IP phones, and printers within each office.
* **Firewalls** help keep the network secure by filtering out unwanted traffic and threats from outside the organization. Currently, only the Dallas office has one.

**Network Strengths and Weaknesses**

Overall, the network works, but there are some weak spots. Especially when looking ahead to future growth.

* If the connection between the Dallas and Memphis routers goes down, Memphis users could lose access to email, HR systems, and other shared resources located in Dallas. Communication tools like video calls and VoIP may also stop working between offices.
* The Memphis office only has one switch and one router, which is risky. If either device fails, the entire office could go offline.
* While the Dallas office has a firewall for protection, Memphis does not, making it more vulnerable to cyber threats or unauthorized access.

**Physical Network Devices**

The network at SNHUEnergy uses a bunch of important gadgets:

* **Routers:** They connect Dallas, Memphis, and the main office to each other through VPNs on the internet.
* **Switches:** Handle the local traffic inside each office, connecting computers, printers, and servers.
* **Firewalls:** Keep the Dallas and HQ safe by filtering traffic, but Memphis ain't got one yet.
* **Access Points:** Lets people connect to the network wirelessly.
* **Servers:** Run the important apps like SQL databases and VoIP servers, which are mostly at the HQ.
* **Endpoints:** All the computers, phones, laptops, and printers that people use everyday.

**Critical Traffic Patterns**

Important types of traffic zooming around their network:

* **Voice over IP (VoIP):** Voice calls get managed through special protocols and most of the action goes through HQ.
* **Application Traffic (SQL):** People in Dallas and Memphis talk to the main SQL database sitting at HQ.
* **Network Management Traffic:** IT guys use SNMP and RDP to manage devices remotely.
* **Other Traffic:** File sharing and logging in happens over SMB and LDAP protocols.

**Patterns Across the Infrastructure**

* Both Dallas and Memphis hook up to HQ using VPN tunnels.
* SQL database queries and VoIP calls all go through HQ.
* Remote management like RDP happens from HQ out to the branch offices.

Because everything goes through HQ, it’s kind of like a choke point, which could be a bad thing if the company keeps growing.

**Performance Issues**

Here’s some stuff that might go wrong if they don't fix it:

* **VPN Bottleneck:** Too much traffic could clog up the VPNs, slowing down everything.
* **Latency and Jitter:** Real-time things like VoIP and video calls might get choppy.
* **Single Point of Failure:** If HQ goes down, everyone else is stuck.
* **Bandwidth Saturation:** Growing more without getting bigger pipes will make everything slower.

**Example:** If too many people are working at the same time in Memphis, their payroll app might crash or get super slow.

**Security Issues**

Big security risks if they keep rolling like this:

* **Memphis Office Vulnerability:** No firewall means hackers might just walk right in.
* **HQ Compromise Risk:** If something bad happens at HQ, every office is at risk.
* **Weak VPN Security:** If the VPNs aren't locked down real good, attackers could snoop on data.
* **No Backup Links:** One path means no plan B if it fails.

**Example:** A hacker could attack Memphis' router, then creep into the whole network since they don’t have enough defenses.

**Visual Representation**

A diagram visual representation of the output of the traffic flows in the project.

A diagram of a computer network

AI-generated content may be incorrect.

**Future Network Architecture**

**Future Communication Needs**

As SNHUEnergy grows, it will need:

* Faster, more reliable connections between offices for calls and meetings.
* Stronger support for remote work.
* A network that can grow without slowing down.
* Backup systems to keep things running even if one part fails.
* Better protection for data and systems.

**Network Architecture Recommendation**

**Proposed Design**

The new plan includes:

* **SD-WAN:** Replacing old VPNs with smarter, more reliable SD-WAN connections.
* **Cloud services:** Moving apps like email and collaboration tools to the cloud.
* **Backup data center:** Setting up a second location or using cloud backup.
* **Zero trust security:** Tighter controls for who can access what.
* **Upgraded firewalls and monitoring:** Adding better firewalls and security tools at all sites.
* **Dedicated connections:** Using private, high-speed links where it makes sense.
* **Wi-Fi 6:** Upgrading office Wi-Fi for better speed and coverage.

**Why It’s Better:**

* **More reliable:** SD-WAN and better connections mean fewer dropped calls and faster data access.
* **Cloud ready:** Employees can access tools from anywhere without putting extra load on the HQ.
* **Safer:** Zero trust and upgraded firewalls help keep hackers out.
* **Always on:** Backups and failovers make sure the company stays online even if one site goes down.

**Future Visual Representation**

A diagram of a fire safety system

AI-generated content may be incorrect.

**Planning and Security**

**Mitigating Performance and Security Issues**

To resolve issues like VPN congestion and high latency, SNHUEnergy should move away from traditional VPNs and adopt SD-WAN. This upgrade enables smarter routing decisions, better bandwidth efficiency, and centralized control. From a security standpoint, introducing a zero-trust model—focusing on least-privilege access and identity verification—will ensure that only verified users and devices can reach sensitive parts of the network.

Adding backup data routes and integrating cloud-based failover systems will help prevent disruptions caused by single points of failure. At the device level, deploying endpoint detection and response (EDR) solutions will bolster defense by identifying and mitigating threats early. Each office location should also be protected with next-generation firewalls (NGFWs), which offer deep traffic inspection and advanced threat prevention.

**Recommended Network Management Tool**

SolarWinds Network Performance Monitor (NPM) is suggested to monitor network performance in real-time. It provides visibility into latency, bandwidth use, and device health, allowing the IT team to catch and resolve problems proactively before they escalate.

**Recommended Security Devices**

1. **Next-Generation Firewalls (NGFWs):** Installed at every site to monitor application-level traffic, enforce policies, and block malicious activity.
2. **Intrusion Detection and Prevention Systems (IDS/IPS):** Used to identify unusual traffic patterns and automatically respond to potential threats.
3. **Multi-Factor Authentication (MFA) Gateways:** Helps prevent unauthorized access, even if login credentials are compromised.
4. **Endpoint Detection and Response (EDR):** Protects user devices from ransomware, phishing, and other malicious actions.

**Necessary Changes to Existing Devices**

* Routers need to support SD-WAN functionality and compatible routing protocols.
* Switches may require firmware upgrades or replacement to support proper network segmentation.
* Existing firewalls should be upgraded to NGFWs that support deep packet inspection.
* Current VPN hardware should be reconfigured or replaced with cloud-ready secure edge solutions.

**Implementation Challenges and Solutions**

* **Downtime Risks:** Minimize disruption with phased rollouts during off-peak hours and use temporary parallel systems when needed.
* **Training Needs:** Provide IT staff with onboarding sessions and vendor-supported training for SD-WAN and new security tools.
* **Budget Limitations:** Prioritize upgrades in the most vulnerable areas (like Memphis) and implement enhancements in phases.

**Risks of Not Updating**

If SNHUEnergy does not modernize its network, it will remain exposed to serious threats like ransomware, data breaches, and compliance violations. Operational downtime could increase, and an attack on a site like Memphis could damage the company’s reputation, lead to customer distrust, financial penalties, and widespread service disruption.

**References**

Southern New Hampshire University. (2025). *IT 640 Final Project Scenario*. SNHU. <https://snhu-media.snhu.edu/files/course_repository/graduate/it/it640/it640_final_project_scenario.pdf>

uCertify. (n.d.). *Chapter 2: Networking basics*. <https://www.ucertify.com/app/?func=ebook&chapter_no=2#top>

uCertify. (n.d.). *Chapter 3: OSI model*. <https://www.ucertify.com/app/?func=ebook&chapter_no=3#top>

uCertify. (n.d.). *Chapter 3: Protocols and standards*. <https://www.ucertify.com/app/?func=ebook&chapter_no=3#076jw>

uCertify. (n.d.). *Chapter 10: Network security*. <https://www.ucertify.com/app/?func=ebook&chapter_no=10#top>

uCertify. (n.d.). *Chapter 11: Troubleshooting and monitoring*. <https://www.ucertify.com/app/?func=ebook&chapter_no=11#top>

Mitchell, C. (2021, April 13). *Near the heart of Silicon Valley, a community failed by the big internet providers is building its own network*. <https://ilsr.org/articles/near-the-heart-of-silicon-valley-a-community-failed-by-the-big-internet-providers-is-building-its-own-network/>

Krebs, B. (2023, January 19). *New T-Mobile breach affects 37 million accounts*. <https://krebsonsecurity.com/2023/01/new-t-mobile-breach-affects-37-million-accounts/>

uCertify. (n.d.). *Chapter 16: Common Security Concepts*

<https://www.ucertify.com/app/?func=ebook&chapter_no=17#top>

uCertify. (n.d.). *Chapter 17: Common Type of Attacks*

[*https://www.ucertify.com/app/?func=ebook&chapter\_no=18#top*](https://www.ucertify.com/app/?func=ebook&chapter_no=18#top)

uCertify. (n.d.). *Chapter 18: Network Hardening Techniques*

[*https://www.ucertify.com/app/?func=ebook&chapter\_no=19#top*](https://www.ucertify.com/app/?func=ebook&chapter_no=19#top)

uCertify. (n.d.). *Chapter 19: Remote Access Methods*

[*https://www.ucertify.com/app/?func=ebook&chapter\_no=20#top*](https://www.ucertify.com/app/?func=ebook&chapter_no=20#top)

uCertify. (n.d.). *Chapter 20: Physical Security*

[*https://www.ucertify.com/app/?func=ebook&chapter\_no=21#top*](https://www.ucertify.com/app/?func=ebook&chapter_no=21#top)