**Wireless Network Design Report**

**Somali Health Data Exchange (SHDX).**

**Course: Wireless and Mobile Technology**

**Student Name: Abdullahi Ahmed Mohamud**

**Student ID: MDC220004**

**Table of Contents**

1. Introduction
2. Design Methodologies
	* Top-Down Approach
3. Design Phases
	* Planning Phase
	* Design Phase
	* Implementation Phase
	* Testing and Validation
4. Tools and Techniques

**1. Introduction**

**1.1 Definition and Importance**

Wireless network design for the Somali Health Data Exchange (SHDX) involves the strategic planning, selection, and implementation of network components to create a robust and interconnected digital health infrastructure. This network is tailored to meet specific requirements such as comprehensive coverage across diverse geographic regions, high capacity to handle large volumes of health data, scalability to accommodate future growth, and stringent security measures to protect sensitive health information.

Importance of Somali health data exchange:

A well-designed wireless network ensures reliable communication across health institutions in Somalia. This is crucial for seamless data exchange and real-time access to patient records, which facilitates timely and coordinated medical interventions. Consistent connectivity is essential for the continuous operation of health services, especially during emergencies where any delay can have significant consequences.

Optimizing network performance is vital for the efficient transmission of large health datasets, such as medical images and patient records, reducing wait times and enhancing the overall efficiency of healthcare delivery. Minimizing latency supports critical applications like telemedicine, where real-time communication between healthcare providers and patients is necessary for effective consultations and treatment.

The network design also supports future growth by providing a scalable infrastructure that can accommodate the expansion of health services and the integration of new health institutions. This scalability ensures that SHDX can grow in response to increasing healthcare demands. Furthermore, the infrastructure is designed to support the adoption of emerging technologies such as IoT-based health monitoring and advanced diagnostic tools, thereby future-proofing the health data exchange and ensuring ongoing improvements in healthcare delivery.

Enhancing security is a key aspect of the network design, with strong protocols in place to protect sensitive health data from unauthorized access and cyber threats. This is crucial for maintaining patient confidentiality and trust in the health system. The network design also adheres to international and local standards and regulations for health data security, ensuring compliance with legal and ethical requirements.

Facilitating efficient resource allocation is another important benefit of a well-designed network. The network enables real-time monitoring of health resources, such as blood banks and medical supplies, ensuring that they are distributed efficiently based on current needs. This supports optimized logistics and resource management, reducing waste and improving the overall efficiency of the healthcare system.

Lastly, a robust wireless network improves public health outcomes by enabling enhanced data analytics and better understanding of public health trends. This supports proactive health interventions and policy-making. Effective disease surveillance and outbreak management are also facilitated by the network, allowing for rapid response to public health threats.

the importance of wireless network design for the Somali Health Data Exchange cannot be overstated. It ensures reliable communication, optimizes performance, supports future growth, enhances security, facilitates efficient resource allocation, and improves public health outcomes. This robust digital health infrastructure is critical for transforming healthcare delivery in Somalia and achieving better health outcomes for the population.

The Somali Health Data Exchange (SHDX) aims to create an interconnected health data network across Somalia by centralizing health data, SHDX ensures efficient resource allocation and improved public health monitoring, allowing for prompt responses to health crises. Economically, the wireless network reduces infrastructure costs and supports future expansions, making it a cost-effective solution. Socially, it fosters healthier, more productive communities. The scalable infrastructure accommodates new technologies, ensuring long-term improvements and maintaining the healthcare system's technological edge. Overall, SHDX aims to significantly improve healthcare outcomes and socio-economic development in Somalia.

**2. Design Methodologies**

The Somali Health Data Exchange (SHDX) is dedicated to addressing the fragmented nature of health data collection and management in Somalia by interconnecting health institutions at regional and national levels. A primary user need is centralized health data access. Health institutions require a platform that consolidates patient data, birth registration information, and blood bank resources into a single, easily accessible system. This centralization is vital for efficient data management and improved patient care outcomes.

Real-time data sharing is another critical user need. Health professionals must be able to share and receive health data promptly to ensure timely interventions and coordinated care. This capability is essential for responding to emergencies and managing ongoing patient care effectively. The SHDX aims to provide a robust system that supports instantaneous data exchange among health institutions.

Security is paramount in the exchange of health data. Users need assurance that sensitive health information is protected during transmission and storage. Advanced encryption methods and secure login protocols are necessary to safeguard this data. Compliance with international data protection regulations and also Somali data protection authority will also be a priority to maintain user trust and legal adherence.

Reliable connectivity is another essential need for health institutions using the SHDX. The platform must be supported by a robust wireless infrastructure that ensures consistent and uninterrupted access to e-health services. This reliability is critical for maintaining continuous data flow and avoiding disruptions in patient care.

Scalability is a key consideration for the SHDX. As the number of health institutions and the volume of health data grow, the system must be able to scale accordingly. This scalability will ensure that the platform remains effective and responsive to the evolving needs of Somalia's healthcare sector.

Interoperability is also necessary for the SHDX to function effectively. The infrastructure must be compatible with existing hospital infrastructures to facilitate smooth connectivity and transmission. This compatibility will minimize disruption and ensure that health institutions can easily adopt and benefit from the new platform.

To ensure the effective use of the SHDX, comprehensive training and ongoing technical support are essential. Health institutions need guidance on how to navigate and utilize the new e-health services. Continuous support will help address any issues that arise and ensure that users can fully leverage the platform's capabilities.

The SHDX also aims to enhance public health monitoring and resource allocation. By providing a centralized and interconnected platform, the organization can facilitate better tracking of health trends and more efficient distribution of resources. This improved coordination will ultimately lead to better healthcare outcomes for the population. In the near future, SHDX plans to expand its solutions within the health sector by assisting hospitals in building digital infrastructure to become smart hospitals. Additionally, SHDX aims to help these hospitals host their systems in the SHDX data center, allowing them to access their systems with low latency.

Overall, the business goals of the SHDX focus on creating a unified and efficient health data exchange system that addresses the current gaps in Somalia's healthcare infrastructure. By meeting the needs of health institutions and ensuring reliable, secure, and scalable solutions, the SHDX aims to improve patient care, enhance public health monitoring, and optimize resource allocation across the nation. In conjunction with these goals, the expansion into digital infrastructure and smart hospital development signifies a commitment to futureproofing the healthcare system and ensuring that health institutions can operate at the forefront of technological advancements.

This forward-thinking approach not only addresses immediate needs but also prepares the healthcare sector for future challenges and opportunities. By building smart hospitals and providing low-latency access through the SHDX data center, health institutions will be better equipped to deliver high-quality care efficiently. This initiative will also support the digital transformation of the healthcare system, making it more resilient and adaptable.

* **Conceptual Design for SHDX Network Architecture**

The Somali Health Data Exchange (SHDX) aims to establish a robust and efficient network architecture to interconnect health institutions at regional and national levels. This architecture is designed to facilitate seamless data exchange, improve care coordination, and enhance public health monitoring. The network will leverage advanced wireless technologies and a resilient topology to ensure high availability, security, and scalability.



**Network Architecture Details**

* In this network architecture, redundancy and reliability are key objectives. The design incorporates multiple layers of redundancy to ensure continuous operation even in the event of hardware failures. The core components of the network include FortiGate firewalls, Cisco Catalyst switches, Dell servers, and Ubiquiti NanoStation devices.

**Firewall and Router Configuration**

* At the heart of the network's security and routing functions are two redundant FortiGate 600F devices. These FortiGate units serve dual roles as both routers and firewalls. They manage traffic routing with one upstream connection and provide comprehensive security features to protect against threats. The redundancy ensures that if one FortiGate unit fails, the other can seamlessly take over, maintaining network integrity and security.

 **Distribution and Access Layer**

* The distribution and access layers of the network are built using two redundant Cisco Catalyst 9300 series switches. These switches are known for their high performance, reliability, and scalability, making them ideal for both distribution and access functions. The redundancy of the switches ensures continuous network availability, as the failure of one switch does not disrupt the network operations. These switches also support advanced features such as stacking and high-speed connectivity, enhancing the overall network performance.

**Server Deployment**

* Two Dell R7 servers are deployed to provide essential network services. These servers are initially configured to handle DNS services and network monitoring tools, such as Zabbix. DNS services are crucial for translating human-readable domain names into IP addresses, ensuring smooth network navigation. Zabbix, an advanced monitoring tool, helps in tracking network performance, detecting issues, and ensuring optimal operation of the network infrastructure.

**Wireless Connectivity**

* For the wireless connection between the SHDX data center and hospital data centers, the NanoStation M5 AC devices from Ubiquiti are used. These devices are chosen for their low cost, high performance, and small form factor, making them extremely versatile and economical to deploy. The NanoStation M5 AC supports high-speed data transmission over long distances, ensuring reliable connectivity between disparate locations. This is crucial for maintaining seamless communication and data exchange between health

|  |  |  |  |
| --- | --- | --- | --- |
| Device name | Model | Quantity  | Description |
| FortiGate firewall | 600F Series NGFW | 2 | The FortiGate 600F Series NGFW combines AI-powered security and machine learning to deliver Threat Protection at any scale. Get deeper visibility into your network and see applications, users, and devices before they become threats. |
| Cisco switch | Catalyst 9300 Series | 2 | The Cisco Catalyst 9300 Series switches are the next generation of enterprise-class stackable access-layer switches that are part of the Catalyst 9000 switching family. These switches support full PoE+, Cisco UPOE, and field-replaceable redundant fans and power supplies. In addition, Cisco Catalyst 9300 Series models also support a variety of fixed and modular uplink options for both copper and fiber uplink support as well as dense 1GE fiber connectivity for FTTX and 1GE aggregation. |
| Dell server | PowerEdge R760 | 2 | Dell PowerEdge R760 is a 2U, two-socket rack server. Gain the performance you need with this full-featured enterprise server, designed to optimize even the most demanding workloads like Artificial Intelligence and Machine Learning.Add up to two Next Generation Intel® Xeon® Scalable processors with up to 56 cores for faster and more accurate processing performance. |
| Nano station | Ubiquiti nano station m5 ac | 2 | Indoor/outdoor, high-performance CPEs featuring airMAX® AC technology and a dedicated Wi-Fi radio for management, frequency: 5 GHz, throughput: 450+ Mbps, range: 15+ km, 2 x Gigabit Ethernet Port, PoE PSU, 802.3af Support. |

* institutions and the SHDX central system.

**Detailed Design**

Access Point Locations:

One NanoStation M5 AC will be installed on the roof of the SHDX data center to serve as the central access point. Each hospital data center will also have one NanoStation M5 AC installed on the roof or an elevated position to establish a direct line of sight with the SHDX data center.

Frequency Channels:

To minimize interference and maximize performance, the 5 GHz frequency band will be used for all NanoStation M5 AC devices. This band is less congested than the 2.4 GHz band and supports higher data rates, which is crucial for maintaining reliable and high-speed connections across multiple health institutions. The specific channels within the 5 GHz band will be selected based on local spectrum availability to ensure minimal overlap and interference.

**Security Settings:**

Encryption: All NanoStation M5 AC devices will use WPA2-AES encryption to secure wireless communications.

Authentication: Access to the wireless network will be restricted using a strong, unique pre-shared key (PSK) for each device.

Firewall Rules: Access points will be configured with firewall rules to limit access to authorized devices and protect against unauthorized intrusions.

MAC Address Filtering: Each NanoStation M5 AC will employ MAC address filtering to allow only pre-approved devices to connect to the network.

Monitoring and Alerts: The Zabbix network monitoring tool will be configured to monitor the status and performance of each NanoStation M5 AC, providing real-time alerts for any security incidents or performance issues.

By leveraging these advanced wireless technologies and secure configurations, SHDX aims to create a resilient, scalable, and secure network architecture that will support the efficient exchange of health data and improve healthcare outcomes across Somalia.

**3. Design Phases**

**3.1 Planning Phase**

* **Site Surveys**

The tool used for site surveying is the UISP Design Center by Ubiquiti. This tool is preferred for its comprehensive features that allow detailed planning and optimization of wireless networks. UISP Design Center provides a virtual environment to simulate and assess network performance, measure signal strength, identify obstacles, and map coverage areas. Its user-friendly interface and precise data make it an invaluable resource for planning complex network architectures like the SHDX.



In the provided image, the UISP Design Center displays the planned deployment of a NanoStation M5 AC access point at the SHDX data center. The access point (AP2) is positioned at coordinates 2.034262, 45.242 with an antenna gain of 19 dBi and a channel width of 100 MHz. The expected signal strength at this location is -38 dBm, with a capacity of 1.07 Gbps over a distance of 1.15 km to the station (Station2), which is positioned at coordinates 2.041636, 45.290015. The height of AP2 is set at 32.85 meters with an azimuth of 7° and a tilt of 1.46°, ensuring optimal signal propagation towards the target station.

**Spectrum Analysis**

Analyzing the radio frequency spectrum is critical to ensure optimal channel selection and minimal interference. The UISP Design Center tool provides detailed insights into available channels and potential interference sources. By scanning the spectrum, planners can identify suitable channels for each NanoStation M5 AC device, focusing on the 5 GHz band. Channels like 36, 44, 149, 157, and 165 are evaluated for their current usage and interference potential. This process ensures optimal performance with minimal overlap and interference, supporting efficient and reliable health data exchange across Somalia's healthcare institutions.

**Traffic Estimation**

Estimating network traffic is essential for ensuring the SHDX network meets user and application demands. Analyzing user behavior and application requirements, such as accessing patient records and conducting video consultations, helps determine bandwidth needs. For instance, with 20 institutions and 10% of users engaged in high-bandwidth activities, the total bandwidth required during peak usage is calculated as follows:

20 institutions × 5 high-bandwidth users/institution × 5 Mbps/user=500 Mbps

This ensures the network can handle approximately 500 Mbps during peak times, providing smooth and uninterrupted service.

**3.2 Design Phase**

In the SHDX network design, a collapsed core architecture is utilized to integrate the core and distribution layers, enhancing efficiency and reducing complexity.

**Core and Distribution Layer:** The core and distribution functions are managed by two redundant FortiGate 600F devices. These devices serve as both routers and firewalls, ensuring high-speed data transfer and robust security. They are responsible for managing traffic between the SHDX data center and the connected health institutions, providing centralized control and seamless data routing.

**Access Layer:** The access layer is handled by two redundant Cisco Catalyst 9300 series switches. These switches connect end devices, such as computers and IoT devices, to the network. They ensure reliable and high-performance connectivity across the network, distributing data efficiently to various access points and maintaining network integrity through redundancy.

**Link Budget Analysis**

Link Budget Analysis

Conducting a link budget analysis is essential to ensure that the SHDX network has sufficient signal strength for reliable communication. This involves calculating the link budget by considering factors such as transmit power, antenna gain, and path loss.

Transmit Power:

The NanoStation M5 AC devices have a maximum transmit power of 25 dBm. This high transmit power ensures strong signal transmission over long distances, which is crucial for maintaining reliable connectivity between the SHDX data center and hospital data centers.

Antenna Gain:

The NanoStation M5 AC features a built-in antenna with a gain of 16 dBi. This high gain helps to focus the signal in a specific direction, enhancing the signal strength over long distances and improving the overall link quality.

Path Loss:

Path loss refers to the reduction in signal strength as it travels from the transmitter to the receiver. Several factors affect path loss, including the distance between the access point and the station, environmental obstacles, and frequency used. In the SHDX network, the typical distance between the data center and the hospital data centers is around 1.15 km. Using the 5 GHz frequency band, which is less susceptible to interference but more affected by physical obstructions, accurate path loss calculations are necessary.

This analysis ensures that even with a link budget of -55.6 dB, the network can maintain reliable communication. The strong antenna gain and proper placement help mitigate the path loss, ensuring robust connectivity. By thoroughly performing link budget analysis, SHDX can ensure optimal signal strength and reliable data exchange across its healthcare network.

**3.3**

**Implementation Phase**

* **Equipment Selection**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device name | Model | Quantity  | Description | Software |
| FortiGate firewall | 600F Series NGFW | 2 | The FortiGate 600F Series NGFW combines AI-powered security and machine learning to deliver Threat Protection at any scale. Get deeper visibility into your network and see applications, users, and devices before they become threats. | FortiOS |
| Cisco switch | Catalyst 9300 Series | 2 | The Cisco Catalyst 9300 Series switches are the next generation of enterprise-class stackable access-layer switches that are part of the Catalyst 9000 switching family. These switches support full PoE+, Cisco UPOE, and field-replaceable redundant fans and power supplies. In addition, Cisco Catalyst 9300 Series models also support a variety of fixed and modular uplink options for both copper and fiber uplink support as well as dense 1GE fiber connectivity for FTTX and 1GE aggregation. |

|  |
| --- |
| Cisco IOS XE |

|  |
| --- |
|  |

 |
| Dell server | PowerEdge R760 | 2 | Dell PowerEdge R760 is a 2U, two-socket rack server. Gain the performance you need with this full-featured enterprise server, designed to optimize even the most demanding workloads like Artificial Intelligence and Machine Learning.Add up to two Next Generation Intel® Xeon® Scalable processors with up to 56 cores for faster and more accurate processing performance. | VMware ESXi, Windows Server, Zabbix |
| Nano station | Ubiquiti nano station m5 ac | 2 | Indoor/outdoor, high-performance CPEs featuring airMAX® AC technology and a dedicated Wi-Fi radio for management, frequency: 5 GHz, throughput: 450+ Mbps, range: 15+ km, 2 x Gigabit Ethernet Port, PoE PSU, 802.3af Support. | airOS 8, UNMS (Ubiquiti Network Management System) |

* **Installation Guidelines**

FortiGate Firewalls (600F Series NGFW)

Physical Installation:

1. Unpack and Inspect:

 - Unbox the FortiGate firewall and check all components for any damage.

 - Ensure the package includes rack mount brackets, power cables, and necessary screws.

2. Rack Mounting:

 - Attach the rack mount brackets to the firewall using the provided screws.

 - Slide the firewall into the designated rack space and secure it with rack screws.

 - Ensure proper ventilation to prevent overheating.

3. Power Connection:

 - Connect the power cable to the firewall and plug it into a UPS or stable power source.

 - Turn on the firewall using the power button.

Configuration:

1. Initial Setup:

 - Connect a console cable from your PC to the firewall's console port.

 - Use a terminal emulator (e.g., PuTTY) to access the firewall's command line interface.

 - Log in with the default credentials (username: admin, password: leave blank) and configure the initial network settings, including IP addresses and gateways.

 - Access the web interface via the configured IP address to continue setup.

2. Firmware Update:

 - Download the latest firmware from the Fortinet support site.

 - Upload and install the firmware through the web interface by navigating to the System > Firmware section.

3. Security Policies and Logging:

 - Configure security policies to control network traffic.

 - Enable logging and monitoring features to track network activity and ensure security.

 Cisco Catalyst Switches (9300 Series)

Physical Installation:

1. Unpack and Inspect:

 - Unbox the Cisco switches and verify all components are intact.

 - Ensure the package includes rack mount brackets, power cables, and necessary screws.

2. Rack Mounting:

 - Attach the rack mount brackets to the sides of the switch using the provided screws.

 - Securely mount the switch in the rack space, ensuring proper cable management.

3. Power Connection:

 - Connect the power cable to the switch and plug it into a UPS or stable power source.

 - Turn on the switch using the power button.

Configuration:

1. Initial Setup:

 - Connect to the switch console port using a console cable and a terminal emulator.

 - Access the switch's command line interface to configure initial settings, including hostname and management IP address.

 - Save the configuration and verify connectivity to the management network.

2. Firmware Update:

 - Download the latest firmware from the Cisco support site.

 - Upload and install the firmware through the console or web interface.

3. VLAN and QoS Configuration:

 - Create VLANs to segment network traffic and enhance security.

 - Configure Quality of Service (QoS) settings to prioritize critical traffic such as voice and video.

Dell PowerEdge Servers (R760)

Physical Installation:

1. Unpack and Inspect:

 - Unbox the Dell servers and check all components for any damage.

 - Ensure the package includes rack mount rails, power cables, and necessary screws.

2. Rack Mounting:

 - Attach the rack mount rails to the sides of the server using the provided screws.

 - Securely mount the server in the designated rack space.

 - Connect power supplies and network cables.

3. Power Connection:

 - Connect the power cables to the servers and plug them into a UPS or stable power source.

 - Turn on the servers using the power button.

Configuration:

1. Initial Setup:

 - Access the server BIOS/UEFI during the boot process by pressing the appropriate key (e.g., F2).

 - Configure initial settings such as date, time, and boot order.

 - Save changes and exit BIOS/UEFI.

2. Operating System Installation:

 - Insert the Proxmox VE installation media (USB/DVD) and boot from it.

 - Follow the on-screen instructions to install Proxmox VE.

 - Configure network settings and IP addresses as required.

3. Virtual Machine and Application Setup:

 - Access the Proxmox VE web interface to create and manage virtual machines.

 - Install and configure applications such as Zabbix for network monitoring and DNS services.

Ubiquiti NanoStation M5 AC

Physical Installation:

1. Unpack and Inspect:

 - Unbox the NanoStations and verify all components are intact.

 - Ensure the package includes mounting brackets, PoE injectors, and necessary cables.

2. Mounting:

 - Mount the NanoStations on rooftops or elevated positions using the provided mounting kits.

 - Ensure the devices are securely fastened and aligned for optimal line-of-sight communication.

 - Run Ethernet cables through weatherproof conduits to protect against environmental factors.

3. Power Connection:

 - Connect the Ethernet cable from the NanoStation to the PoE injector.

 - Plug the PoE injector into a stable power source.

Configuration:

1. Initial Setup:

 - Access the NanoStation configuration interface by connecting to the built-in Wi-Fi radio or Ethernet port.

 - Open a web browser and enter the default IP address (192.168.1.20) to access the web interface.

2. Firmware Update:

 - Download the latest firmware from the Ubiquiti support site.

 - Upload and install the firmware via the web interface.

3. Network Configuration:

 - Set up network settings, including IP addresses and SSIDs.

 - Configure the devices for point-to-point (PtP) or point-to-multipoint (PtMP) links as required.

 - Use the airView spectrum analyzer to optimize channel selection and minimize interference.

4. Performance Optimization:

 - Adjust the transmit power and antenna alignment to maximize signal strength.

 - Monitor the link quality and performance using the built-in diagnostic tools.

By following these detailed installation and configuration guidelines, the SHDX network will be set up for optimal performance, security, and reliability. This robust infrastructure will support the seamless exchange of health data across Somalia's healthcare institutions.

**3.4 Testing and Validation**

* **Testing the Network**
	+ Test the network to ensure it meets design specifications and performance requirements.
	+ Example: Conduct throughput tests, coverage tests, and security assessments.

**Still working on this step, conducting throughput tests, coverage tests, and security assessments to ensure the network meets design specifications and performance requirements.**

**References**

* List all references and sources used in the preparation of the report in APA format.

<https://www.healthit.gov/topic/health-it-and-health-information-exchange-basics/what-hie>

Rudin, R. S., Motala, A., Goldzweig, C. L., & Shekelle, P. G. (2014). Usage and Effect of Health Information Exchange: A Systematic Review. *Annals of Internal Medicine*, *161*(11), 803. <https://doi.org/10.7326/M14-0877>

Menachemi, N., Rahurkar, S., Harle, C. A., & Vest, J. R. (2018). The benefits of health information exchange: An updated systematic review. *Journal of the American Medical Informatics Association*, *25*(9), 1259–1265. <https://doi.org/10.1093/jamia/ocy035>

Kiourtis, A., Mavrogiorgou, A., Kyriazis, D., Graziani, A., & Torelli, F. (2020). Improving Health Information Exchange through Wireless Communication Protocols. *2020 16th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 32–39. <https://doi.org/10.1109/WiMob50308.2020.9253374>