Secure On-demand Health Services

Video Presentation:
https://uowmailedu-my.sharepoint.com/:f:/r/personal/aas208_uowmail_edu_au/Documents/STUDY%20SEMESTER/Spring%20Semester%2023/CSIT985%20-%20Strategic%20Network%20Design/Video%20Presentation?csf=1&web=1&e=96So3A

Table of Contents

1. Executive summary

The case study of Secure On-demand Health Services (SOHS) sheds light on a revolutionary change in the provision of community healthcare. Traditional healthcare silos have been dismantled with an emphasis on patient needs, opening the door for a collaborative approach including a wide range of medical specialists. This novel approach seeks to provide fair access to specialised healthcare services for all community members by extending their reach beyond regional limitations.

The need to deliver secure healthcare services in the context of this redesigned healthcare environment is the main issue this case study attempts to solve. The need for safe, on-demand healthcare services is growing as community health standards do. Patients should have access to specialised healthcare resources regardless of where they are or when they become sick.

Leading this change is SOHS, which places a strong emphasis on the integration of interdisciplinary healthcare professionals and dismantles obstacles that prevent people from accessing healthcare. The case study emphasises how vital it is to guarantee that everyone using this innovative paradigm may access it safely.

Policymakers and healthcare professionals can learn a great deal about the future of community healthcare by looking at the SOHS case study. This paradigm, which breaks down the conventional boundaries of healthcare services and prioritises patient needs, establishes a new benchmark for the delivery of healthcare by emphasising security and inclusivity. The SOHS case study is a vital resource that emphasises the significance of safe, on-demand healthcare services that are available to everyone as the sector develops.

2. Introduction

In the ever-evolving landscape of healthcare, the Secure On-demand Health Services (SOHS) case study emerges as a pioneering exploration into the future of community healthcare delivery. With rising standards and an unwavering focus on patient needs, the traditional paradigms of healthcare delivery are rapidly shifting. This transformation is characterized by a departure from siloed medical services towards a collaborative, multidisciplinary approach involving doctors and allied healthcare professionals.

In today's healthcare scenario, where access to specialized services often depends on geographical location and appointment schedules, the need for a paradigm shift is glaring. The SOHS case study mirrors this pressing reality, highlighting the urgent need to break down these barriers. By dismantling the constraints of time and place, SOHS envisions a healthcare system that is truly accessible to all, ensuring that no one is left behind when it comes to essential medical services.

Possible Outcomes: Empowering Communities and Ensuring Security

At the heart of the SOHS case study lies the potential to empower communities. By leveraging the collective expertise of diverse healthcare professionals, this innovative model promises specialized healthcare services that are tailored to individual needs. Patients, regardless of their location, socio-economic status, or the complexity of their medical conditions, stand to benefit from this holistic approach. Through seamless collaboration and information sharing, the case study foresees a future where healthcare services are not just reactive but proactive, addressing underlying health issues before they escalate.

Moreover, the emphasis on security within this model is pivotal. SOHS stands as a beacon of secure healthcare delivery. The case study outlines robust measures to protect patient data, ensuring confidentiality and compliance with healthcare regulations. By prioritizing security, SOHS aims to build trust among patients, enabling them to seek medical assistance without fear of compromising their privacy.

Futuristic Scenarios: A Glimpse into Tomorrow's Healthcare Landscape

Looking ahead, the SOHS case study hints at futuristic scenarios that could revolutionize healthcare delivery on a global scale. One such scenario is the widespread adoption of telemedicine and virtual consultations. With advancements in technology, patients might have the option to consult specialists from the comfort of their homes, transcending geographical boundaries.

Additionally, predictive analytics and artificial intelligence could play a pivotal role in healthcare. Such a scenario not only enhances patient outcomes but also contributes significantly to reducing the burden on healthcare systems.

Furthermore, the integration of wearable devices and smart technologies into healthcare could lead to a continuous, real-time monitoring of patients. This not only provides valuable data for healthcare professionals but also empowers individuals to actively manage their health, fostering a culture of preventive care.

3. Development

a. Analysis and Specification Document

i. Initial Conditions

Analyzing the given case study, it's clear that Secure On-demand Health Services (SOHS) is a group of four General Practitioner (GP) practices in the Sydney area looking to collaborate and provide a wider range of specialized health care services. The primary goal is to deliver secure, on-demand health services to the community, breaking down traditional healthcare silos and improving patient access to specialized services. In this analysis, we will identify requirements from the interview with the Chief Information Officer (CIO) of SOHS and gather additional requirements as needed.

The insights gleaned from the interview with the Chief Information Officer (CIO) of Secure On-demand Health Services (SOHS) provide a profound understanding of the unique challenges and needs of the organization. Addressing these requirements comprehensively is crucial to the success of the network design.

1. Limited Technical Knowledge:

The CIO’s limited technical expertise underscores the importance of creating an intuitive network infrastructure. User-friendliness becomes paramount. The interfaces, dashboards, and overall system architecture must be designed with simplicity in mind. Intuitive navigation and minimal technical jargon will empower the CIO and other non-technical staff to effectively manage the network without undue complexity.

2. Broadband Technologies:

The emphasis on utilizing broadband technologies highlights the centrality of high-speed, reliable internet connections in SOHS's operations. The network must be robust enough to handle substantial data traffic, especially during telehealth consultations and video conferences. Redundancy in internet connections could be explored to ensure uninterrupted services. Moreover, Quality of Service (QoS) mechanisms should be implemented to prioritize real-time data transmission, guaranteeing smooth telemedicine encounters.

3. Secure Network:

The need for a secure network architecture cannot be overstated. Safeguarding sensitive patient information is paramount, requiring robust encryption protocols, firewall configurations, and intrusion detection systems. Multi-factor authentication can add an extra layer of security, ensuring that only authorized personnel can access critical data. Regular security audits and updates will be necessary to fortify the network against evolving cyber threats.

4. Collaboration Among GPs:

Facilitating seamless communication and data sharing among the collaborating General Practitioners (GPs) is pivotal. A unified communication platform, integrating secure messaging, video conferencing, and file sharing, should be implemented. This will enable GPs to consult each other in real-time, share expertise, and exchange patient information securely. Moreover, access controls should be finely tuned, allowing GPs to access only the relevant patient data based on their specialization.

5. Geographical Separation:

Overcoming the geographical challenge of the 13-kilometer separation between the GP practices requires innovative solutions. Virtual Private Network (VPN) technology can create a secure, encrypted tunnel over the internet, connecting the geographically dispersed practices as if they were on the same local network. Additionally, leveraging cloud-based services can enhance collaboration, enabling practitioners to access shared resources and applications regardless of their physical location.

6. Access to Specialized Services:

The network's ability to support on-demand access to specialized medical services is paramount to SOHS's mission. Implementing a cloud-based service delivery model can ensure scalability and flexibility. Specialized services such as imaging, pathology, psychology, plastic surgery, and treatment for various medical conditions can be hosted on cloud servers. This not only ensures rapid scalability based on demand but also centralizes the management of these services, making updates and maintenance more efficient.

7. Storage and Access to Historical Health Records:

Securing historical health records mandates a robust and redundant data storage solution. Implementing a combination of on-premises servers and cloud-based storage can provide the necessary redundancy. Regular backups, both on-site and off-site, are vital to prevent data loss. Implementing data access policies, along with audit trails, ensures that patient records are accessed only by authorized personnel. Additionally, the deployment of Blockchain technology can enhance the integrity and immutability of patient records, providing an additional layer of security and trustworthiness.

8. IP Address Range:

Integrating the provided IP address ranges into the network design demands meticulous planning. Proper addressing and routing are fundamental to ensure that data packets reach their intended destinations accurately. Network Address Translation (NAT) and dynamic routing protocols can be employed to manage the internal and external IP address ranges effectively. This meticulous allocation ensures efficient utilization of IP addresses while allowing for seamless communication within the internal network and with external entities.

ii. Requirements Specification and Map

In addition to the specific requirements gathered from the interview with the Chief Information Officer (CIO) of Secure On-demand Health Services (SOHS), several additional aspects need to be considered to ensure a comprehensive and future-proof network design.

1. Scalability:

Scalability is a fundamental requirement for SOHS's network. As the organization expands or integrates new specialized services, the network infrastructure must be capable of accommodating increased data traffic and additional users. Scalability ensures that the network remains responsive and efficient, even in the face of growing demands. Implementing scalable technologies, such as cloud-based services and virtualization, allows SOHS to seamlessly expand its operations without compromising performance.

2. Redundancy:

Redundancy measures are vital to guarantee uninterrupted service delivery. Implementing backup internet connections and failover mechanisms ensures that if one connection fails, traffic can be seamlessly redirected to an alternate path. Redundancy not only enhances reliability but also minimizes downtime, thereby preserving the continuity of critical healthcare services, especially during emergencies or network failures.

3. Quality of Service (QoS):

Quality of Service (QoS) mechanisms play a pivotal role in prioritizing critical medical data. Telemedicine and video conferencing require low latency and high bandwidth to ensure real-time communication. By implementing QoS, SOHS can prioritize these services, ensuring a seamless and responsive experience for both healthcare professionals and patients. Prioritizing traffic based on its importance ensures that essential medical data receives precedence over less time-sensitive data, enhancing the overall efficiency of the network.

4. Compliance:

Adherence to healthcare data security and privacy regulations is non-negotiable. SOHS must comply with relevant regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States or similar regulations in Australia. Ensuring compliance involves implementing robust security protocols, data encryption, access controls, and audit trails. Regular compliance audits and updates are essential to align the network design with the ever-evolving regulatory landscape.

5. Training and Support:

Given the CIO's limited technical knowledge, providing comprehensive training and ongoing support for staff is imperative. Training programs should cover network management, troubleshooting procedures, and best practices for ensuring network security. Additionally, establishing a dedicated support system, including helpdesk services and online resources, can empower staff to address network-related issues promptly and effectively. A well-informed team can enhance the overall efficiency and security of the network.

6. Interoperability:

Interoperability is essential for seamless communication and data exchange between SOHS's network and existing healthcare IT systems, external healthcare providers, and organizations. Ensuring compatibility with diverse systems and standards allows for the effortless transfer of patient data, fostering collaboration and continuity of care. Interoperability promotes a unified healthcare ecosystem, enabling efficient sharing of information while preserving data integrity and security.

7. Data Backup and Recovery:

Robust data backup and recovery solutions are paramount to prevent data loss and ensure business continuity in case of disasters. Regular automated backups of critical data, both on-site and off-site, coupled with a well-defined recovery plan, safeguard against potential data loss due to system failures, cyberattacks, or natural disasters. Implementing versioning and data deduplication further optimize storage space and enhance the efficiency of backup processes.

8. Secure Remote Access:

Enabling secure remote access is essential in the modern healthcare landscape. Authorized users, including healthcare professionals and staff, must be able to securely access the network and its resources remotely. Implementing Virtual Private Network (VPN) technologies, multi-factor authentication, and encrypted communication channels ensures that remote access remains secure. Secure remote access facilitates telecommuting, enabling healthcare professionals to provide consultations and access patient records securely from any location, enhancing flexibility and service availability.

9. Monitoring and Analytics:

Implementing robust network monitoring and analytics tools is essential for proactive issue identification and resolution. Real-time monitoring allows IT administrators to identify potential bottlenecks, security threats, or performance issues promptly. Analytics tools provide valuable insights into network usage patterns, enabling data-driven decision-making. By proactively addressing issues and optimizing network performance, SOHS can ensure a seamless and reliable user experience.

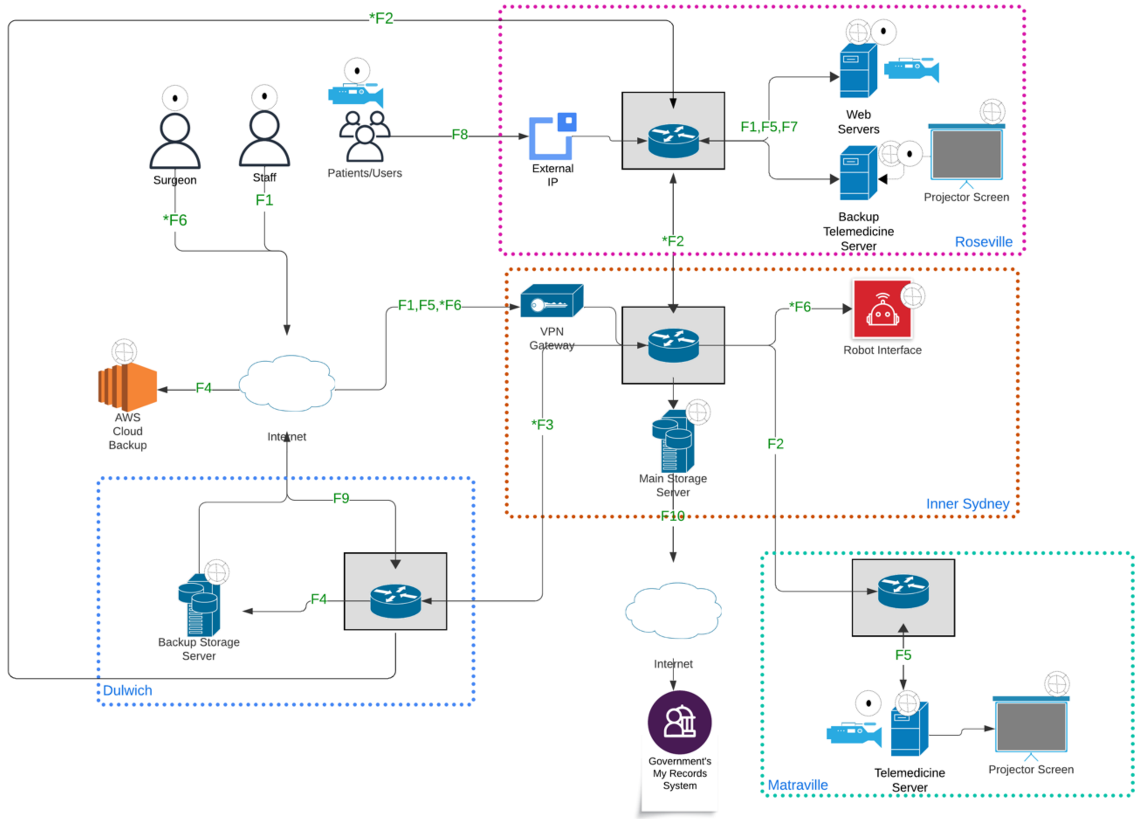
10. Budget Constraints:

Considering budget constraints is a practical necessity in any network design endeavor. Prioritizing cost-effective solutions without compromising quality is essential. Conducting a thorough cost-benefit analysis can help identify areas where investments yield the most significant impact. Open-source software, cloud-based services, and virtualization technologies often provide cost-effective solutions without compromising functionality or security. Regular evaluation of budget allocations ensures that resources are optimally utilized, striking a balance between functionality, security, and financial considerations.

Incorporating these additional requirements into the network design not only ensures a robust and future-proof infrastructure but also aligns SOHS with industry best practices. By addressing scalability, redundancy, quality of service, compliance, training, interoperability, data backup, secure remote access, monitoring, and budget constraints, SOHS can establish a network that not only meets the immediate needs but also adapts and evolves in response to the dynamic healthcare landscape, providing high-quality, secure, and accessible healthcare services to the community.

It is safe to say that, the network design for SOHS should address not only the technical requirements but also consider the user-friendliness, security, and compliance aspects, especially given the CIO's limited technical knowledge. The geographical separation of the practices, the need for secure data access, and the provision of specialized services make this a complex project that requires careful planning and execution. The additional requirements identified here will help create a robust and future-proof network design that supports the mission of Secure On-demand Health Services.

iii. Flow Analysis



SOHS Flow Diagram

The above diagram gives a comprehensive overview of all the flows identified for the creations of SOHS network. These flow are marked from F1 to F10. Critical flows are marked with *.

F1. Staff Remote Access to SOHS Services:

- Flow: Remote Location (Staff Home) → VPN Gateway → Internal Network (Access to required services)
- Purpose: Staff accessing the internal network securely to provide services, access records, or any other internal resource.

F2. Inter-office Communication:

- Flow: One GP office → Interconnecting Router/Switch → Another GP office
- Purpose: Sharing of patient records, consultations between doctors in different offices, administrative communication, etc.
- Type: Critical

F3. Accessing Patient Records:

- Flow: Any GP Office → Inner Sydney Database Server
- Purpose: Retrieval of patient history, updating records after new consultations, etc.
- Type: Critical

F4. Backup Processes:

- Flow 1: Inner Sydney Database Server → Backup Server in another office
- Flow 2: Inner Sydney Database Server → Cloud Backup Service
- Purpose: Regular backup of patient data for redundancy and disaster recovery.

F5. Telemedicine Consultation:

- Flow: Patient Location → Telemedicine Server in the respective GP office (which then can communicate with other offices if required)
- Purpose: HD quality video consultations, possibly involving multiple doctors from different locations.

F6. Interactive Surgical Robots Operation:

- Flow: Remote Surgeon Location → VPN Gateway → Inner Sydney Site's Robot Interface
- Purpose: Performing surgeries remotely with real-time controls and feedback.
- Type: Critical

F7. Web-Based Services for Staff (emails, social media, etc.):

- Flow: GP Office → Internet Gateway → Web Services
- Purpose: Allowing staff to access personal emails, social media, etc., without compromising the integrity and security of the internal network.

F8. Public Access to SOHS Web Services:

- Flow: Public Internet → SOHS Web Servers
- Purpose: Patients accessing services, booking consultations, viewing records, or any other provided online service.

F9. Communication with Backup Cloud:

- Flow: Backup Server at Office → Internet Gateway → Cloud Service in Australia
- Purpose: Storing encrypted backups in the cloud as an additional layer of data redundancy.

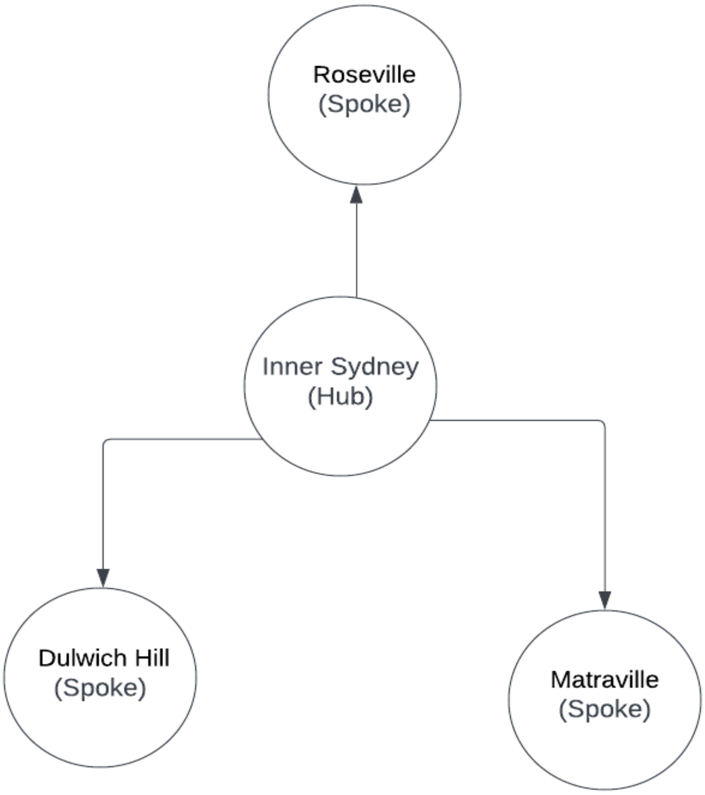
F10. Communication with Government's My Records Initiative:

- Flow: Inner Sydney Database Server → Internet Gateway → Government's My Records System
- Purpose: Complying with government regulations for patient data availability.

b. Reference Architecture

i. Architectural models

1. Hub and Spoke/ Star Model:



Hub and Spoke Topology

The Hub and Spoke model is structured around a central location known as the hub. For SOHS, the main office in Inner Sydney would act as this hub. This hub is essentially the nucleus of the network, with all other sites (the GP practices in this scenario) referred to as the spokes. Importantly, these spokes connect directly to the hub and not with each other.

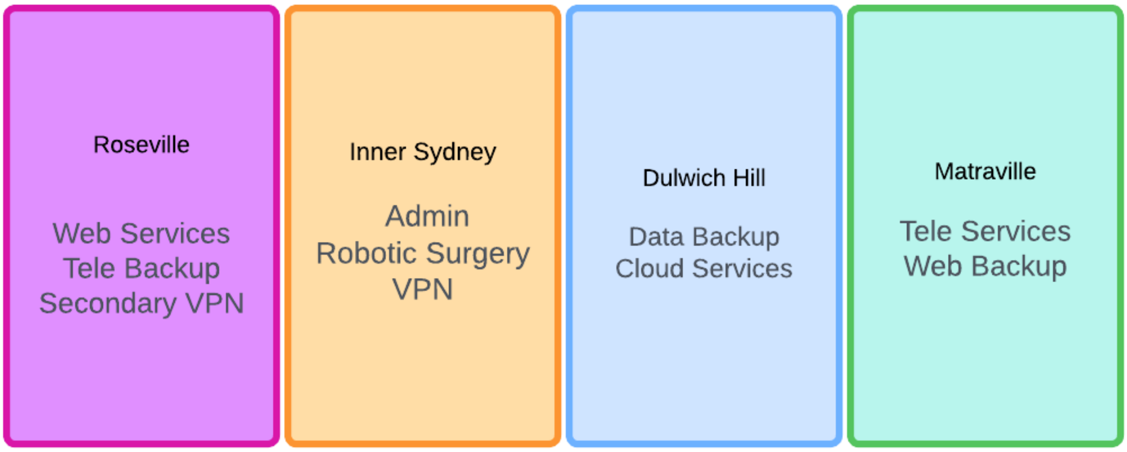
Advantages:

- Efficiency: This model streamlines the paths that need oversight, facilitating easier network monitoring and management.
- Centralization: It offers centralized services. By placing key resources and functionalities at the hub, the model can lead to both cost savings and operational efficiency.

Disadvantages:

- Single Point of Failure: The major downside is its vulnerability to hub failures. If the hub experiences issues or goes offline, all the spokes lose connectivity.
- Potential Congestion: With inter-site traffic required to pass through the hub, there's a risk of congestion, especially during peak times.

2. Service-Oriented Model:



Service Model Based Breakdown of Network Functions

The Service-Oriented Model prioritizes network design based on the services offered rather than merely physical locations or topology. In the context of SOHS, the network would be divided into distinct service zones, such as Telemedicine, Surgical Robots, Database & Backup, Staff Access, and Web Services.

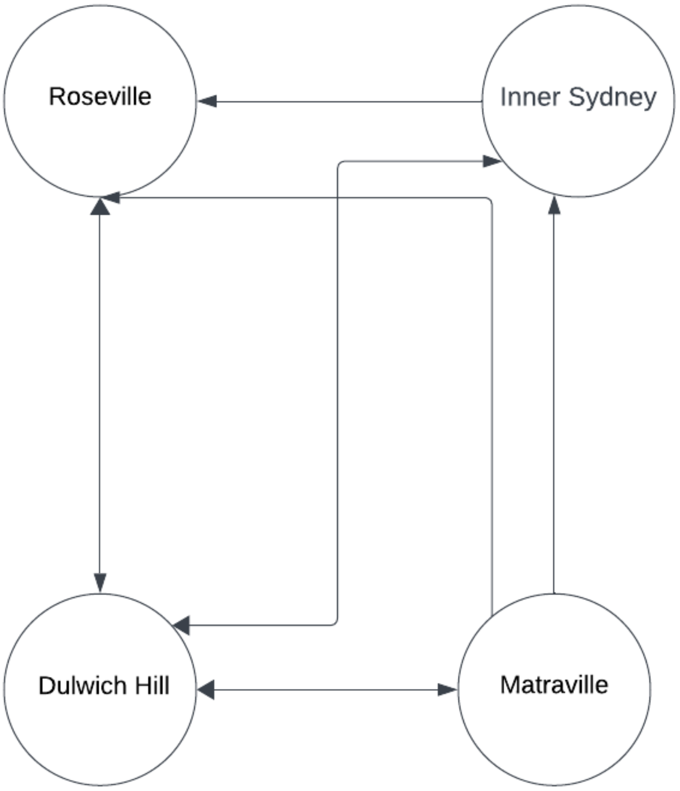
Advantages:

- Specialized Service Delivery: This model is tailored to ensure smooth delivery of specialized services. Each zone is specifically optimized for its traffic patterns and requirements.
- Enhanced Security: By segregating services, the model facilitates the implementation of service-specific policies and security protocols. This structure inherently boosts the overall security posture of the network.

Disadvantages:

- Resource Intensive: The nature of this model might necessitate more resources, both in terms of hardware and management. This could lead to increased overheads.
- Inter-Service Communication: Communication between different service zones needs meticulous planning. Without proper management, there's a risk of creating bottlenecks or inefficient routing paths.

3. Mesh Model:



Mesh Topology

Every site is interconnected to every other site. This provides multiple paths for data transfer, offering redundancy.

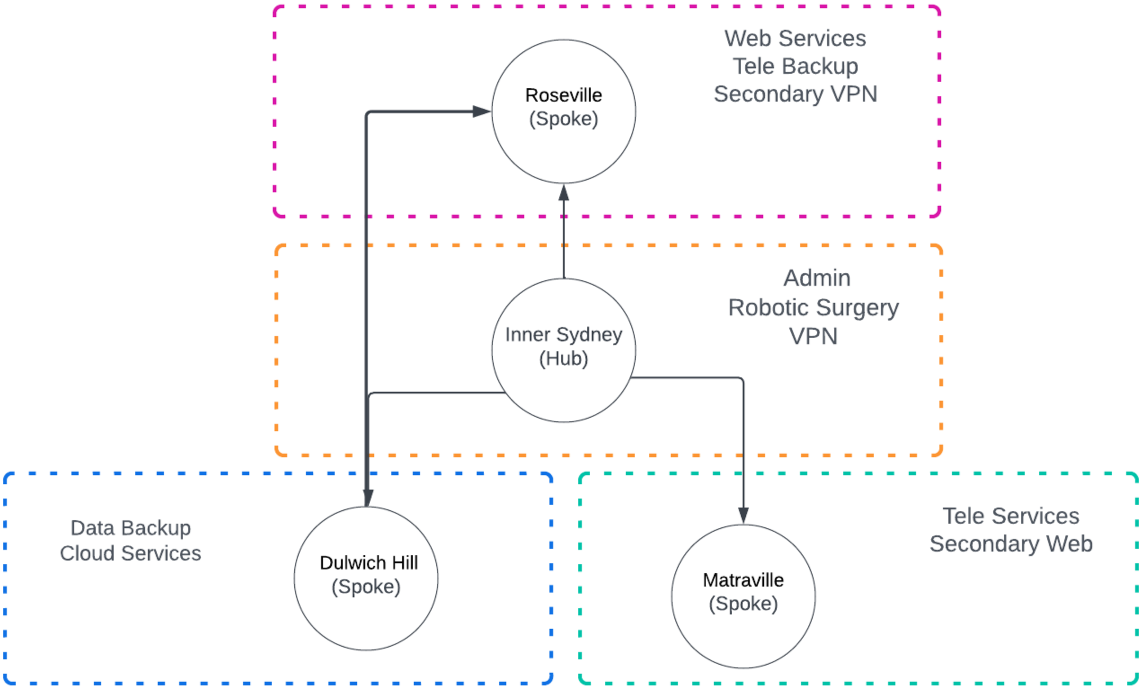
Advantages:

High redundancy. If one link fails, there's an alternative path for data transfer.
Fault tolerance is high due to multiple connections.
Better load balancing as traffic can be routed through the least busy or shortest path.

Disadvantages:

Can be complex and expensive to cable and configure due to the numerous connections.
Management might become challenging as the network grows.

Model in SOHS



Hybrid Topology

Given the critical nature of some of SOHS's services, such as online surgeries, having a redundant connection ensures that there's no service disruption. While the hub and spoke can cater to the primary traffic, a mesh between key sites (like between two major GP practices) can act as a failover mechanism.

While both architectures offer advantages, the best approach for SOHS might be a Hybrid Architecture. They could primarily employ the Hub and Spoke model, with the Inner Sydney office acting as the hub. However, for critical services and backup purposes, key sites can be interconnected in a mesh form. This ensures efficient use of resources while also providing redundancy and fault tolerance.

ii. Addressing and Routing

a. Subnetting:

Subnetting the provided IP range allows for efficient use of IP addresses, avoiding wastage and ensuring room for future expansion. Given there are 4 offices, each office has its dedicated IP subnet, ensuring easy identification and management.

1. Internal IP Subnetting (Range: 172.16.0.0/12)

The ‘/12’ range provide 1048574 addresses which we can divide into 4 subnets as follows:

1. Inner Sydney:

- Starting Address: 172.16.0.0
- Subnet Mask: 255.255.240.0 or /20
- Usable Addresses: 172.16.0.1 to 172.16.15.254
- Broadcast Address: 172.16.15.255
- Provides 4096 IP addresses

2. Roseville:

- Starting Address: 172.16.16.0
- Subnet Mask: 255.255.240.0 or /20
- Usable Addresses: 172.16.16.1 to 172.16.31.254
- Broadcast Address: 172.16.31.255
- Provides 4096 IP addresses

3. Dulwich Hill:

- Starting Address: 172.16.32.0
- Subnet Mask: 255.255.240.0 or /20
- Usable Addresses: 172.16.32.1 to 172.16.47.254
- Broadcast Address: 172.16.47.255
- Provides 4096 IP addresses

4. Matraville:

- Starting Address: 172.16.48.0
- Subnet Mask: 255.255.240.0 or /20
- Usable Addresses: 172.16.48.1 to 172.16.63.254
- Broadcast Address: 172.16.63.255
- Provides 4096 IP addresses

2. External IP Subnetting (Range: 203.10.192.0/20)

Given the `/20` range, which provides 4096 IP addresses, we can divide it as follows:

1. VPN Access for Staff:

Given the emphasis on remote access, it's safe to assume that a sizable chunk of IPs may be required for VPN.

- Range: `203.10.192.0/22`
- Provides 1024 IP addresses, plenty for VPN access.
- Usable Addresses: `203.10.192.1` to `203.10.195.254`

2. Web Servers for Patient Services:

Likely portals for patients to login, check records, or communicate.

- Range: `203.10.196.0/23`
- Provides 512 IP addresses, plenty for clustering and load balancing.
- Usable Addresses: `203.10.196.1` to `203.10.197.254`

3. Telemedicine:

HD teleconferencing, especially for medical applications, might need dedicated IP addresses for better management and prioritization.
- Range: `203.10.198.0/23`
- 512 IP addresses, which can be used for dedicated telemedicine systems and redundancy.
- Usable Addresses: `203.10.198.1` to `203.10.199.254`

4. Backup Cloud Access:

If cloud backups are being taken, these will require IP addresses to communicate securely with the cloud provider.
- Range: `203.10.200.0/24`
- 256 IP addresses should be sufficient for cloud backup communication.
- Usable Addresses: `203.10.200.1` to `203.10.200.254`

5. Miscellaneous Services:

Other potential external-facing services like email servers, DNS, etc.
- Range: `203.10.201.0/24` to `203.10.207.0/24`
- Seven /24 subnets, each providing 256 IP addresses for various services.
- Usable Addresses, for the first subnet: `203.10.201.1` to `203.10.201.254`, and so on.

Office/Area	*Starting Address*	*Subnet Mask*	*Usable Addresses*	*Broadcast Address*
Inner Sydney	172.16.0.0	255.255.240.0	172.16.0.1 to 172.16.15.254	172.16.15.255
Roseville	172.16.16.0	255.255.240.0	172.16.16.1 to 172.16.31.254	172.16.31.255
Dulwich Hill	172.16.32.0	255.255.240.0	172.16.32.1 to 172.16.47.254	172.16.47.255
Matraville	172.16.48.0	255.255.240.0	172.16.48.1 to 172.16.63.254	172.16.63.255
VPN Access for Staff	203.10.192.0	255.255.252.0	203.10.192.1 to 203.10.195.254	
Web Servers	203.10.196.0	255.255.254.0	203.10.196.1 to 203.10.197.254	
Telemedicine	203.10.198.0	255.255.254.0	203.10.198.1 to 203.10.199.254	
Backup Cloud Access	203.10.200.0	255.255.255.0	203.10.200.1 to 203.10.200.254	
Miscellaneous(1/7)	203.10.201.0	255.255.255.0	203.10.201.1 to 203.10.201.254	

Ip table for SOHS network

b. Routing:

Routing is a critical component in any network setup, ensuring that data packets are sent to their appropriate destinations in the most efficient manner. Routing method can be implemented at router level using various routing protocols.

1. Routing Protocols:

OSPF (Open Shortest Path First):

- Overview: OSPF is a link-state routing protocol, which means it uses the state of its links (interfaces) to make routing decisions.
- Advantages: It quickly converges when the network topology changes, making it ideal for a setup where uptime is critical. OSPF supports multiple equal-cost paths, allowing for load balancing.
- Usage in SOHS: OSPF can be used to ensure that data between the main office and GP practices is routed efficiently. Multiple paths can be leveraged to balance the load, especially during peak times.

EIGRP (Enhanced Interior Gateway Routing Protocol):

- Overview: EIGRP is a Cisco proprietary protocol that incorporates the best of both distance-vector and link-state characteristics.
- Advantages: It provides faster convergence than many other protocols due to its use of Diffusing Update Algorithm (DUAL). It also supports unequal path load balancing, which can make better use of redundant paths.
- Usage in SOHS: If the network infrastructure is primarily Cisco, EIGRP might be a good choice. It can help route traffic between GP practices and the central office, taking into consideration different path metrics.

2. Hub and Spoke Topology Implications:

- Predictable Routing Pattern:

The hub and spoke design simplifies the routing table. Since all traffic passes through the hub, routing paths are inherently predictable.

- Centralized Routing:

With the Inner Sydney office acting as the main routing pivot, it becomes the key point for route aggregation and redistribution. This means all GP practices can be efficiently routed via the hub.

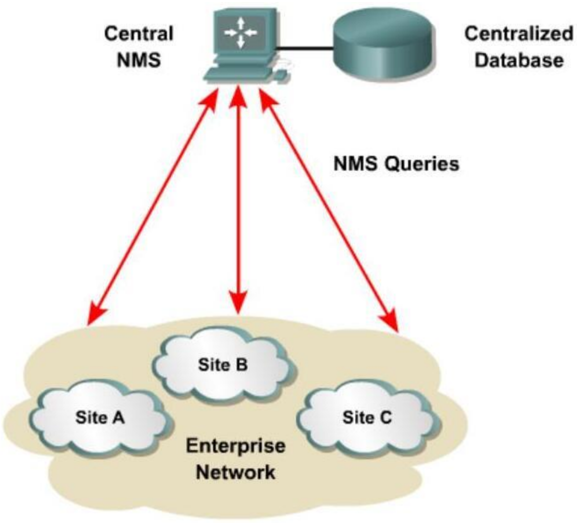
- Resilience and Redundancy:

While the hub and spoke model offers many advantages in terms of routing simplicity, it's essential to ensure that the hub remains highly available. Implementing redundant pathways and possibly a secondary hub can mitigate the risk of a single point of failure.

iii. Network Management Architecture

The modern network demands a seamless and efficient management architecture. Proper network management ensures high availability, fault tolerance, and optimized performance. Given the sensitive nature of services at SOHS, such as surgical robots, the significance of a robust network management architecture cannot be overemphasized. Let's delve deeper into the elements:

1. Centralized Network Management:



Centralized network management consolidates all network management tools and applications in a single location. This enables a holistic view of the network, facilitating easier management, monitoring, and diagnostics.

Advantages:

- Single Pane of Glass:

Centralized NMS offers a unified view of the entire network, enabling faster diagnostics and fault resolution.

- Resource Optimization:

By pooling resources in a single location, there's a reduction in the need for redundant tools and systems across different locations.

- Consistency:

Implementing changes, updates, or policies can be done uniformly across all locations.

- Implications for SOHS:

With the Inner Sydney office acting as the hub, housing the centralized NMS here is logical. It would enable rapid identification of issues across the GP practices and immediate remediation.

2. Remote Monitoring (RMON):

RMON is a standard monitoring specification that enables remote network monitoring of networked devices. This is achieved using agents located on these devices, which then relay information back to the central NMS.

Advantages:

- Enhanced Visibility:

RMON allows for insights into remote network segments without local probes.

- Proactive Management:

It enables the identification of issues before they become critical, thanks to its early warning capabilities.

- Historical Data Analysis:

By gathering data over time, trends can be identified, facilitating predictive management.
Implications for SOHS:

- Implications for SOHS:

For the geographically dispersed GP practices, RMON is invaluable. It ensures that the central NMS in Inner Sydney can efficiently monitor and manage remote segments, ensuring uptime and reliability.

3. VLAN Management:

Virtual Local Area Networks (VLANs) segregate network traffic based on function, department, or project, rather than physical location.

Advantages:

- Efficient Traffic Segregation:

VLANs ensure that only necessary traffic traverses specific network segments, reducing congestion.

- Enhanced Security:

By segregating traffic, unauthorized access across VLANs can be minimized.

- Flexibility:

VLANs can be quickly reconfigured as organizational needs change.

- Implications for SOHS:

Given the varied nature of services at SOHS - from telemedicine to surgical robot operations - the importance of traffic segregation using VLANs cannot be overstated. It ensures that each service gets the necessary network resources and adds a layer of security by isolating potentially sensitive traffic.

iv. Performance Architecture:

The performance architecture of a network is the cohesive and integrated set of components, mechanisms, and policies designed to ensure optimal network performance, response times, and user satisfaction. Given the unique requirements of the SOHS network, considering the criticality of telemedicine and surgical robotics, the following components are fundamental:

1. Quality of Service (QoS):

Quality of Service (QoS) is a set of mechanisms that prioritize network traffic according to predefined criteria to ensure that certain data streams receive higher priority and, thus, better network performance.

Advantages:

- Traffic Prioritization:

Critical applications like HD telemedicine and surgical robots get the necessary bandwidth ensuring real-time, seamless operations.

- Minimized Latency:

Vital for telemedicine consultations and robotic surgeries where real-time data transfer is of the essence.

- Predictable Network Experience:

Ensures consistent quality for end-users irrespective of other network activities.

- Implications for SOHS:

In a healthcare setting, where the difference of a few seconds can be significant, QoS becomes non-negotiable. It ensures that mission-critical applications always have precedence in the network.

2. Load Balancers:

Load balancers distribute incoming network traffic uniformly across multiple servers, ensuring that no individual server is overloaded.

Advantages:

- Even Server Load Distribution:

Prevents server overloads, ensuring optimal server response times.

- Enhanced User Experience:

By efficiently directing traffic, load balancers can reduce waiting times for users.

- Failover Capability:

If one server fails, traffic is redirected to others, ensuring service continuity.

- Implications for SOHS:

Given the potential high volume of patient requests and telemedicine traffic, load balancers are imperative to ensure smooth service delivery without overburdening any individual server.

3. Redundant Links:

Redundancy in network links means having backup pathways for data, ensuring uninterrupted service even if the primary link fails.

Advantages:

- Service Continuity:

Even if a primary link fails, the backup ensures services remain uninterrupted.

- Load Sharing:

Redundant links can be used to share the data load, providing enhanced transmission rates.

- Increased Reliability:

The existence of backup links increases the overall reliability of the network.

- Implications for SOHS:

In the health sector, downtime is not acceptable, especially for critical services like telemedicine. Redundant links guarantee high availability and uptime.

In our network design we have added redundant link between Roseville and Dulwich Hill. Now even if the hub went down the system can be brought up using backups at these locations with minimal downtime.

4. Content Delivery Network (CDN):

CDNs are networks of servers distributed across various locations. These servers store cached versions of static web content, ensuring users access data from the nearest server.

Advantages:

- Optimized Load Times:

Due to data retrieval from a nearby server, website and application load times are drastically reduced.

- Reduced Network Load:

As many requests are handled by the CDN, the primary server experiences less load.

- Scalability:

CDNs can handle spikes in traffic, ensuring smooth user experience even during high traffic times.

- Implications for SOHS:

For web-based services and resources, a CDN can ensure that patients or staff experience fast and reliable access, improving user satisfaction and operational efficiency. Established providers like AWS CloudFront or Cloudinary offer robust CDN services, suitable for various business requirements.

v. Security and Privacy Plan

a. Data Storage:

Since the requirement regarding the data storage is high availability of the data/service, backup, monitoring, scalability, storage in the cloud, security etc, we as a team are inclined towards AWS RDS since AWS RDS provides all the facilities with easy deployment. We need to be familiarized with a few terms before moving forward.

1. AWS Region:

An AWS Region is a geographic area anywhere in the world where the company has a cluster of data centres. The 31 launched AWS Regions are available in all continents except Antarctica. Most AWS Regions are in North America, Europe, and Southeast Asia. The North Virginia AWS Region was the first to launch in 2006 and comprises the most Availability Zones to date (6).

2. AWS Availability Zone:

An AWS Availability Zone refers to one or more data centres that are physically separate and have independent power and cooling yet are linked logically. This design adds layers of resilience (durability, security, and reliability) to the AWS cloud infrastructure. For example, AWS stores your data in multiple Availability Zones in the same or different AWS Regions, so it remains available even if the primary data centre is affected by an outage. This is perfect for backup and disaster recovery purposes.

3. Master Database:

Master database is the primary or source database and supports read and write operations i.e SELECT, INSERT, UPDATE, DELETE operations etc.

4. Slave Database (Replica):

Slave databases, also known as replica databases or secondary databases, are copies of the master database. These replicas are read-only and are used for offloading read traffic from the master database, which certainly helps in stability of the master database and prevents the database from crashing. It hardly takes a few minutes to copy the content from master database to slave database. Slave databases are highly recommended to be in different Availability Zones to prevent application from shutdown because if one of the database instances is affected in one AZ (Availability Zone) then another database instance will be running in different AZ.

5. Replication Process:

Replication process can be both synchronous or asynchronous based on the configuration done by Database Administration. In synchronous configuration, write operations are performed in both master and slave databases at the same time to achieve data consistency whereas in asynchronous configuration, data changes are reflected or written in the master database first and later copied into the slave database which might result in slight delay in the applications that is accessing slave database.

6. Enable Multi-AZ Deployments:

If one of the DB instances fails in any one of the Availability Zone, AWS automatically creates replicas or takes the snapshots and dumps to other DB instances of different Availability Zone. So, deploying slaves in different AZ can be considered as a backup or security.

7. Cross Region Replications:

We cannot control the natural calamities/ natural disasters. Taking this scenario into consideration, cross region replications can be an option if the application supports a vast number of customers or users.

8. Load Balancing:

In any application, read operations are comparatively higher than write operations. So, to balance the read operation, AWS provides ALB (Application Load Balancer) to distribute the read traffic to different slave databases and offload the master database so that the master database can focus on write operation.

Approach:

Since AWS launched AWS Asia Pacific (Sydney) Region in 2012, I could not see a reason to not use AWS for the implementation of this project. Since the network we are planning to build is in Sydney, it is better to use the AWS Asia Pacific (Sydney) region to avoid network latency and achieve requirements like video conferencing etc.
This region has 3 Availability Zones which can be considered for the backup. The approach for backup and recovery that we have decided is master and slave (read replicas in AWS term).

As the requirement states, Master Database will be in Inner Sydney and slave database will be in other remaining Availability Zones. Master Database supports read-write operation whereas slave database supports read-only database. However, the slave database will be updated in no time more like in real time. In addition, we are planning to go ahead with asynchronous configuration in the master slave approach since there will be more reading query or reading operations compared to writing query/operation, the workloads on the master database will be reduced drastically with this approach. On top of that we will be keeping a load balancer to balance the load on each instance of the Database server.

So, if the DB server, let's say slave in one Availability Zone(i.e. Roseville) is not functional due to various reasons i.e. natural calamities or hardware of software issue, AWS automatically will take the snapshot of the master database and load the contents in the standby salve/replica database instance of Roseville Availability Zone since AWS RDS supports Multi-Availability Zone(AZ) deployments.
If the master Database instance located in Inner Sydney goes down, then AWS will conduct a election between the remaining slave database located in different AZ and one of the slave or replica databases is chosen as primary or master database.

b. Security:

Before discussing the Security measure, we believe it is important to understand the malwares and common attacks.

Malware:

Malware is malicious software including

1. Viruses:

Viruses are the software program which inserts itself into other software and can spread from computer to computer. It requires human action or intervention to spread. For instance, let's say you have downloaded a software from the Internet which has a virus and once the software is installed in your system, your system is also infected with a virus. If you then copy that executable program in USB or hard drive and then share it with your friends, those storage devices as well as your friend’s PC are also infected.

2. Worms:

Worms are self-propagating viruses that can replicate themselves provided they have network connectivity. For instance, let’s say your database is infected by worms somehow and the database is connected to multiple other PCs. As long as network connectivity is present, worms can affect the multiple PCs connected to that database.

3. Trojan horses:

Trojan horses are malicious software’s which looks legitimate to trick humans into triggering it. It often installs back doors. For instance, let’s say you are a gamer and while surfing the Internet, you happen to come across the cheat code of any game. On clicking that link, you might get the cheat code. However, trojan horses are installed in your system as well.

4. Ransomware:

It basically encrypts data with the attacker’s key and asks the victim to pay a ransom to obtain the key.

Common Attacks:

1. Script Kiddies:

They are basically low skilled attackers who usually download the script from the Internet and attempt to exploit any vulnerable host they can connect to. These attacks are mostly not targeted against particular individuals or organizations.

2. Targeted Attacks:

They are more skilled than Script Kiddies and aim to exploit particular individuals or organizations.

3. Social Engineering:

The attacker often pretends to be someone they are not by tricking the victim and tries to get the confidential information as much as possible through the telephone or the email. Phishing is a Social Engineering attack where the attacker claims to be the manager or employee of the Company and tries to get the personal information of the victim.

4.DoS (Denial of Service):

DoS prevents actual or legitimate users from accessing the resources from any other servers or hosts by flooding the target system with more traffic than it can handle.

We all know that we need to establish a connection between two hosts before sending sensitive information through the network. The process involved in establishing connection includes host_1 sending a message to host_2, host_2 sending a response back to host_1 and host_1 sending acknowledgement message to host_2 again. This is how the connection between two hosts are established before sending sensitive information through the network.

5. Sniffers:

These attackers usually stay in the middle of the network between the hosts to sniff the data. The attacker can read and modify the data.

c. Security measures:

IDS and IPS (Intrusion Detection System and Intrusion Prevention System):

IDS and IPS analyse packets up to layer 7 of the OSI model looking for the traffic patterns which match known attacks. They can also look for unusual behaviour like normal hosts sending more packets than usual. But sometimes, hosts might have a huge traffic and can send more packets than usual which does not mean that traffic is sent by an attacker. So, to resolve this problem, network administrators need to fine tune IDS and IPS.

However, the positioning of IDS and IPS are different. IDS usually sits alongside the traffic flow and informs security administrators of any potential attacks whereas IPS is positioned inline with the traffic flows and blocks the potential attacks.

Firewalls:

Firewalls are usually deployed on the Internet side or edge and block the potential attacks based on the rules maintained in connection tables which contain a list of source and destination IP address with port number.

Cryptography:

Cryptography transforms readable information into encrypted or unreadable form from one host to another and later decrypted or converted into readable information with the help of a shared key. We need not worry about the sniffers in the network if the sensitive information is encrypted. Cryptography provides Authenticity, Confidentiality, Integrity to our sensitive messages.

1. Symmetric Encryption:

The type of encryption where the same shared key is used to encrypt and decrypt the sensitive information is called Symmetric Encryption. The shared key needs to be kept secret in this type of Encryption. Example: AES, SEAL.

2. Asymmetric Encryption:

The type of encryption where two keys i.e. public key and private key is used to encrypt and decrypt sensitive information respectively. Private key as the name suggests needs to be kept secret unlike public key. Example: RSA, ECDSA.

SSL and TLS (Secure Sockets Layer and Transport Layer Security):
As of now we use TLS since SSL is outdated or deprecated. TLS basically uses symmetric cryptography to encrypt transmitted data. For example: Users share their credit card information in Amazon to purchase through Amazon. That is because Amazon public key or public certificate will be verified by the Certificate Authority (Verisign).

Site-to-Site VPNs:

Site-to-Site VPN network is generally used when we require secure connections between different networks located in different areas but connected over insecure networks such as the Internet. This type of VPN uses symmetric encryption algorithms (AES) to send encrypted traffic over the Internet. There is no need to encrypt the data inside the office since the office network is a trusted network.

Remote Access VPN:
There are multiple applications (like OpenVPN, Cisco AnyConnect) available to achieve Remote Access VPN. Since a home network or hotel network is not considered as a trusted network, employees can use the above-mentioned applications to build a VPN tunnel to access office networks.

1. Split Tunnelling:

In this type of tunnelling, users or employees ought to use a VPN tunnel to access the office network. However, they do not need VPN to access other networks on the internet such as Email, Social networking sites etc.

2. Full Tunnelling:

In this type of tunnelling, users or employees are required to use VPN tunnel to access the office network as well as other networks on the internet such as Email, Social networking sites etc. So, companies have to enforce security policies to limit the sites that employees can access.

Thread defence solutions:

We need to install anti-malware software in all the available host systems. Anti-malware software basically uses signatures to detect malicious software and block it from running. We also need to limit the level access so that employees will not be able to disable the anti-malware software. Also, we can use IPS to detect and block the malwares on the network traffic. For phishing attacks, we need to use ESA (Email Security Appliance) which scans links and attachments in incoming email for malware and spams. We also need to implement policies to prevent sensitive information from being sent out of the organizations. Policies and procedures should be implemented, for example about how and what information can be sent or taken outside the company premises. Moreover, Security awareness training should also be provided to all the employees.
DDos attacks can be prevented either by installing Advanced Firewalls in the network or using quicker connection timeouts and cookies instead of sync Arp connection. All the software needs to be up to date and patched so that it rejects malformed packets.

Line Level Security:

When we receive a Cisco router or switch from the factory, no security is configured at all. We can access the command line via console with no password required. We need to configure it manually so that only the authorized administrators can access the network devices. Minimal password security can be provided to network devices to achieve basic Line Level Security.

1. Console Line Security:

We can configure the router or switch in such a way that it asks for the password when the cable is connected to network devices like router or switch. Only one administrator can connect over a console cable at a time, so the line number is always 0.

2. Virtual terminal VTY line Security:

When the employee or administrator tries to access the networking devices remotely through Telnet or SSH Secure Shell, we can prompt for the password to the administrator. SSH Secure Shell is much more secure than Telnet because all SSH Secure Shell traffic is encrypted whereas Telnet sends the traffic in plain text. So if the attacker is trying to sniff the network traffic, the attacker can see and understand the traffic details along with username and password if we use Telnet.

3. Privileged Exec Mode:

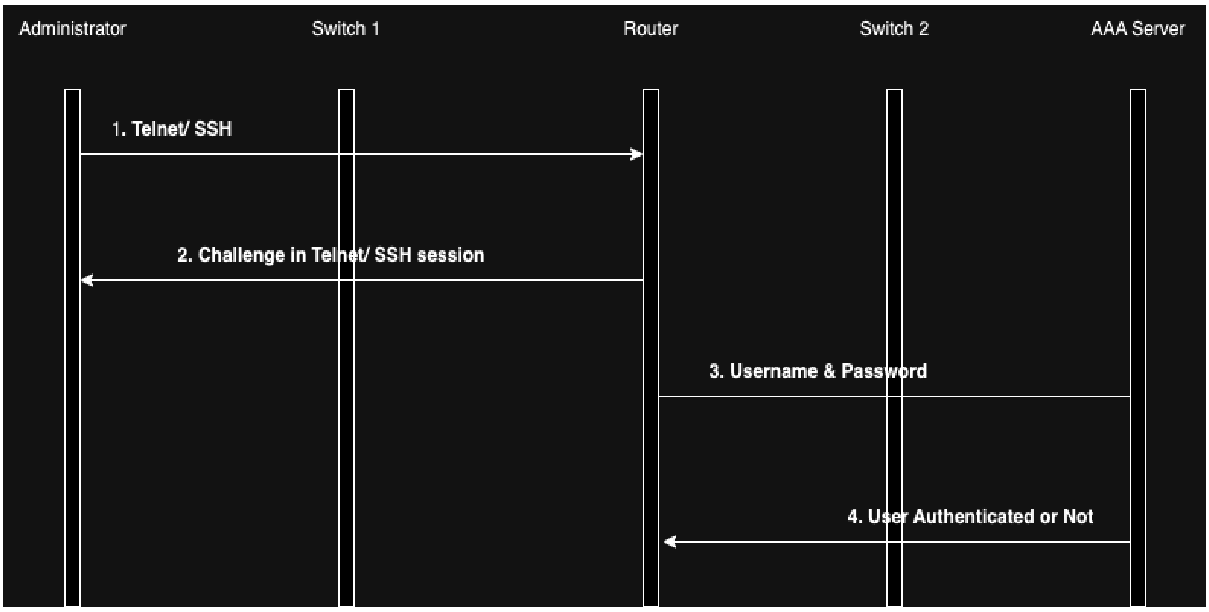
When we want to go from User mode to Privilege Mode, we can configure the networking devices in such a way that it prompts for the password to the administrator.

AAA(Authentication, Authorization and Accounting):

Configuring line level security to all the networking devices is time consuming and frustrating after one point of time. So, it is better to use an external server or AAA server to centralize all the credentials at one place and perform the Authenticity through that server. Authentication verifies somebody is who they claim they are usually by entering username and password. Authorization deals with the access level provided to administrators. Accounting keeps the logs

of all the commands entered by the administrator. Authentication is mandatory whereas Authorization and Accounting is optional.
How AAA works:

Sequence diagram on how AAA works.



The purpose of AAA server is to centralize credentials of all the administrators to one place rather than storing credentials of every administrator in each networking device. When an administrator tries to access Router via Telnet or SSH, Router asks username and password to the administrator. After the administrator provides the credentials i.e username and password, Router redirects entered credentials to AAA server since credentials of all the administrators are stored in AAA server. AAA server verifies the credentials and administrator is either authenticated or not. If the administrator is authenticated, the administrator can see the Router's console and vice versa.

NAT (Network Address Translation)

RFC 1918 specifies private IP address ranges which are not routable on the public internet. Private addresses were originally designed for hosts which should have no internet connectivity because Public IP addresses cost money. If an organization has a part of their network where the hosts need to communicate with each other over IP, but do not require connectivity to the Internet, they can assign private IP addresses.
The designers of IPv4 did not envision the explosive growth of its use. 4.3 billion addresses seemed more than enough. However, the protocol is not particularly efficient in its use of the available space, with many addresses being wasted.
The Internet authorities started to predict address exhaustion in the late 1980's, and IPv6 was developed in the 90's as the long-term solution. IPv6 uses a 128-bit address, compared to IPv4's 32-bit address. However, there is no seamless migration from IPv4 to IPv6.
NAT was implemented as a temporary workaround to mitigate the lack of IPv4 addresses until organizations had time to migrate to IPv6. An organization can use private IP addresses on their inside network, but still grant their hosts Internet access by translating them to their outside public IP addresses. Many industry experts predicted that IPv6 would be extremely popular within a few years. It has not worked as expected since most enterprises today use RFC

1918 IPv4 addresses with NAT. RFC 1918 has the security benefit of hiding the inside hosts by default because they do not have a publicly routable IP address.

1. Static NAT:

Static NAT is a permanent one-to-one mapping usually between a public and private IP address which are basically used for servers which must accept incoming connections.

2. Dynamic NAT:

Dynamic NAT uses a pool of public addresses which are given out on an as needed first come first served basis. Dynamic NAT is usually used for internal hosts which need to connect to the Internet but do not accept incoming connections.

PAT (Port Address Translation):

PAT allows same public IP address to be reused.

Compliance:

AWS Shared Responsibility Approach:

AWS uses a shared responsibility approach model to handle the security in the cloud. Shared responsibility approach includes both AWS and Customer where AWS generally manages and configures the security component of the host operating system and customer manages and configures the security of guest operating system.

AWS is responsible for managing the security of the cloud environment which includes providing a high level of security by hiring the trained security guards in each data centre, 24 hours of surveillance and multi factor authentication to access any control systems. Customers are responsible for managing the security of the content they will store in the services provided by AWS. It is the customer who decides what type of contents are to be stored if the contents need to be encrypted or not and the level of access provided to the end users.

AWS access to customer contents:

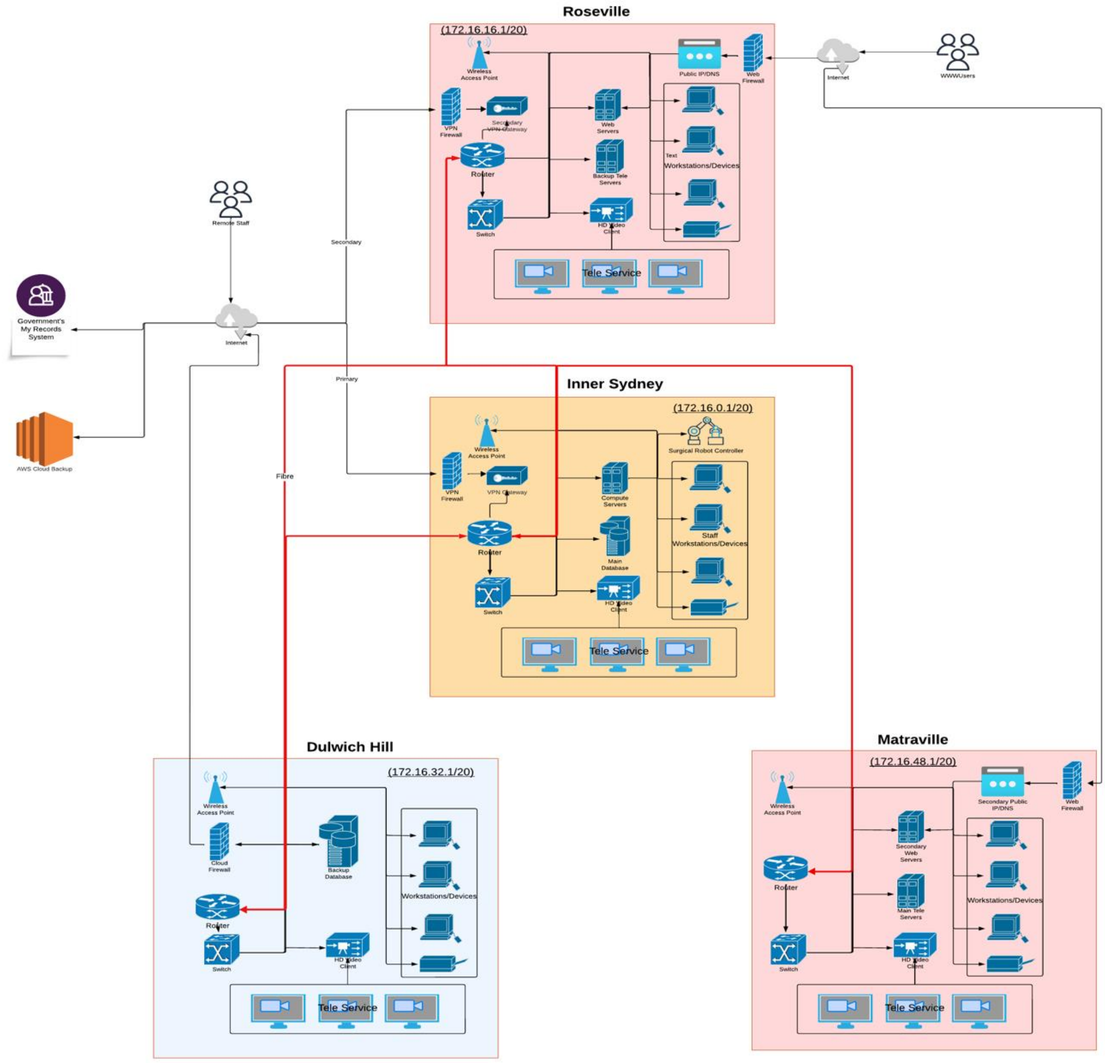
As mentioned above, Customers are responsible for storing the content. AWS does not access the content of the customer unless the consent is provided by the customer himself except legally required. Having said that, if a customer does not trust AWS, the customer can use the encryption feature provided by AWS or the encryption feature provided by a third party.

Government access to customer contents:

AWS does not disclose the content of the customer to the government unless legally required to do so which includes court order and so on.

c. Design Document

i. Topology diagram



First Level Topology diagram for SOHS network

a. Physical Layout:

1. Topology

The physical layout consists of hybrid model composite of star and mesh topology.

- The central hub would be represented by the main office in Inner Sydney.
- Several spokes radiate from the hub, each leading to different GP practices spread across various locations.
- Each GP practice would have its internal networking components like switches, Wi-Fi access points, and possibly a local server.

2. Connections:

- Fiber optic connections link all routers from each site.
- Each router is connected to a switch at its respective site.
- Each switch connects all equipment and servers at its respective site.
- VPN connections established from remote workers to VPN Server located at the Inner Sydney site.
- Secure connection from Dulwich Hill Backup Server to the Cloud Backup.

3. Locations of Key Components:

- Inner Sydney:

- Firewall for protection against external threats.
- A core router connected to other sites.
- A switch connecting all local devices and systems.
- The primary database server containing all patient records.
- Video conferencing equipment.
- Telemedicine Software for surgical robots.

- Roseville, Dulwich Hill, Matraville:

- Firewall at each site.
- Routers at each location to connect them to Inner Sydney and each other.
- Switches at each site to connect local systems.
- Video conferencing equipment at each site.
- Backup Server specifically at the Dulwich Hill site.

- Cloud:

- Cloud-based backup in an Australian data center (AWS) with encrypted patient data.

3. Special Requirements for the Inner Sydney site for the Surgical Robots:

The Inner Sydney site will be the hub of advanced telemedicine services. The following are special considerations:

- Latency & Bandwidth:

Extremely low latency is vital for surgical robot operations. This requires dedicated high-bandwidth lines to ensure that there's no lag during surgical operations.

- Dedicated Subnetwork:

A VLAN (Virtual Local Area Network) should be set up specifically for the surgical robots to isolate their traffic from other network activities, ensuring maximum performance and security.

- Redundancy:

Ensure dual routers and switches at the Inner Sydney site to provide redundancy. If one component fails, the other can take over without interrupting the surgery.

- Backup Power:

Uninterrupted Power Supplies (UPS) and generators to ensure the surgical robots and their networking equipment don't lose power unexpectedly.

- Secure Access:

Only authorized personnel should be able to access the surgical robot systems. This can be achieved using strong authentication methods, like biometrics or smart cards.

- Monitoring & Alerts:

Continuous monitoring of the network performance for the surgical robots. Any minor glitches could lead to complications during surgeries, so instant alerts are crucial for any abnormalities.

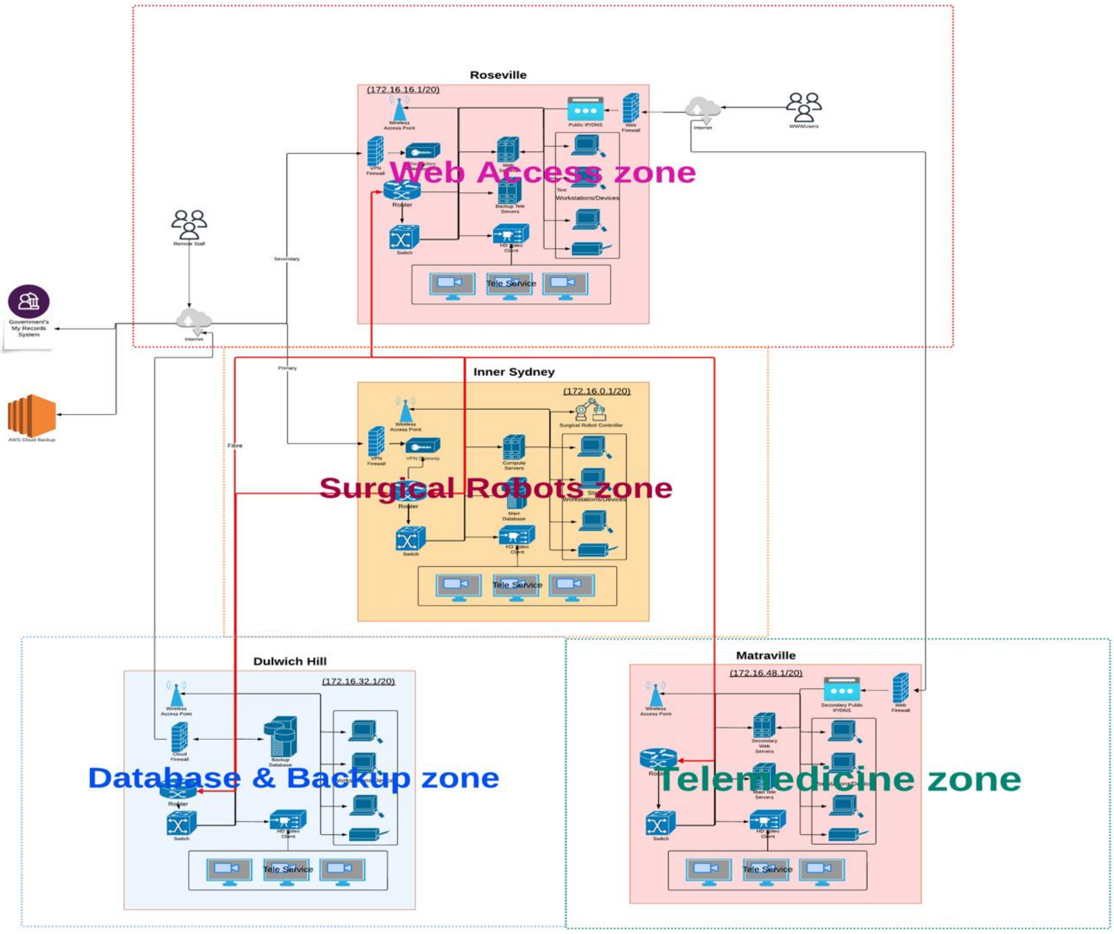
- Quality of Service (QoS):

Implement QoS policies to prioritize the surgical robot's network traffic over other traffic.

- Data Storage:

Real-time storage solutions for surgery recordings, logs, and other data. This is important for post-operation analysis and legal purposes.

b. Logical Layout:



Logical Zones Created based on usage

If the Service-Oriented Model is also incorporated, different zones are created for different purpose:

1. Telemedicine zone:

Focused on video and audio communication systems.

2. Surgical Robots zone:

Prioritizing low latency and high bandwidth.

3. Database & Backup zone:

Emphasizing data security and redundancy.

4. Web Access zone:

To facilitate staff access to the system, possibly VPN connections.
Web Services zone: Managing patient portals, appointment booking systems, etc.

ii. Design Traceability

a. Requirements vs. Design Elements:

1. **Requirement**: Seamless communication between the main office and GP practices.

Design Trace: The Hub and Spoke model chosen ensures a centralized communication system, allowing efficient data sharing and management.

2. **Requirement**: Efficient telemedicine services.

Design Trace: A dedicated telemedicine zone in the Service-Oriented Model, optimized for video and audio streaming.

3. **Requirement**: Secure data transmission for surgical robots.

Design Trace: The surgical robots zone, with enhanced encryption and low-latency pathways.

iii. Design Metrics

Network Uptime:

Given the critical nature of healthcare, the SOHS system should aim for a network uptime of 99.99%. Any downtime could severely affect patient care and medical procedures.

Bandwidth Utilization:

With diverse services like telemedicine and surgical robots, monitoring bandwidth is crucial. The system should ensure that, even during peak times, the bandwidth utilization does not exceed 80%, leaving a 20% buffer.

Latency:

For real-time applications like telemedicine consultations and surgical robots, latency should be kept minimal. A benchmark could be set (e.g., <50ms) to ensure real-time responses.

Security Incidents:

Given patient data's sensitive nature, the SOHS system should employ advanced intrusion detection systems. Metrics would track any unauthorized access attempts or breaches and aim for zero incidents.

Service Availability:

Each service zone, especially critical ones like telemedicine and surgical robots, should have a high service availability rate, say 99.95%. Regular audits would ensure that these services are consistently available without disruptions.

d. Lifecycle consideration

i. Operational suitability

Ensuring a robust service delivery model, especially in the context of high-quality video conferencing and other specified applications, involves a careful blend of technology, processes, and human resources. Here's how you can ensure the service delivery model is robust:

Ensuring a Robust Service Delivery Model for Secure On-demand Health Services (SOHS)
In the dynamic landscape of healthcare, ensuring a robust service delivery model is paramount, especially concerning high-quality video conferencing and other specified applications. This complex task demands a multifaceted approach, integrating cutting-edge technology, meticulous planning, and a relentless focus on user experience.

1. Comprehensive Needs Analysis:

At the core of SOHS's service delivery strategy lies a comprehensive needs analysis. Understanding the specific requirements of healthcare professionals and patients is the foundational step. This analysis delves into the functionalities expected from applications, emphasizing high-quality video conferencing and other essential services.

2. Thoughtful Technology Selection:

The backbone of SOHS's service delivery model is the careful selection of technology solutions. High-quality video conferencing and other applications demand reliable, state-of-the-art technology. Factors such as video quality, encryption capabilities, compatibility across devices, and scalability for future needs are meticulously evaluated.

3. Robust Network Infrastructure:

SOHS invests significantly in a robust network infrastructure. High-speed, reliable internet connections are the lifeblood of seamless communication. Quality of Service (QoS) mechanisms are implemented to prioritize video and real-time data traffic, ensuring minimal latency and a smooth user experience.

4. Stringent Security Measures:

Security is non-negotiable. SOHS implements end-to-end encryption for video conferencing and other applications, guaranteeing the confidentiality and integrity of patient data. Regular updates to security protocols ensure resilience against evolving cybersecurity threats.

5. Scalability and Flexibility:

SOHS designs its systems to be scalable and flexible. The architecture allows for seamless expansion, accommodating the growing number of users or applications. Flexibility is ingrained, enabling the integration of new technologies or applications without disrupting existing services.

6. User-Friendly Interfaces:

A focus on user experience is evident in SOHS's approach. The development of intuitive and user-friendly interfaces for all applications is paramount. Healthcare professionals and patients navigate these applications with ease, fostering a seamless interaction.

7. Comprehensive Training and Support:

SOHS invests in the proficiency of its staff. Comprehensive training sessions are provided to healthcare professionals and support staff, enhancing their confidence and efficiency in using the applications effectively. Ongoing support ensures that any challenges are swiftly addressed.

8. Regular Testing and Quality Assurance:

SOHS adopts a proactive stance through regular testing, simulations, and quality assurance checks. These measures identify glitches or performance issues, which are promptly addressed to maintain the high standard of service.

9. Redundancy and Disaster Recovery:

The importance of redundancy and disaster recovery cannot be overstated. SOHS implements backup internet connections and failover mechanisms, ensuring uninterrupted service delivery even in the face of network failures. A robust disaster recovery plan is in place, swiftly restoring services in unforeseen circumstances.

10. Compliance and Regulations:

Adherence to healthcare data security and privacy regulations is a cornerstone of SOHS's service delivery model. Applications are meticulously audited to maintain compliance with standards such as HIPAA, ensuring patient data remains secure and confidential.

11. Cultivating Continuous Improvement:

Within SOHS, a culture of continuous improvement prevails. Regular assessments of the service delivery model, coupled with feedback mechanisms from healthcare professionals and patients, drive enhancements. The organization remains adaptive, evolving with technological advancements and user needs.

In embracing these principles, SOHS not only ensures a robust, high-quality, and secure healthcare service experience but also cements its position as a reliable partner in the community's healthcare journey. Through innovation and excellent commitment, SOHS stands as a beacon of exceptional service delivery in the healthcare sector.

ii. Supportability

1. Application Requirements for High-Quality Video Conferencing and Real-time Services:

High-Quality Video Conferencing:

a. Adaptive Streaming:

Implement adaptive streaming technology to adjust video quality based on users' internet connection speeds. This ensures optimal quality without interruptions, even when internet conditions fluctuate.

b. Background Noise Reduction:

Integrate noise reduction algorithms to eliminate background noise during video consultations, enhancing the clarity of audio communication between healthcare professionals and patients.

c. Virtual Waiting Rooms:

Include virtual waiting rooms where patients can securely wait for their appointments. Notifications can inform them about their queue status, reducing anxiety and improving the overall patient experience.

d. Language Support:

Provide language options within the video conferencing application, enabling real-time translation services for patients who speak languages different from the healthcare professionals.

e. Session Recording:

Enable the option to record video consultations securely. Stored recordings can serve as valuable references for healthcare providers and patients and can be integrated into the patients' electronic health records with their consent.

2. Real-time Services:

a. Telemedicine Apps Integration:

Seamlessly integrate telemedicine applications, enabling patients to initiate video consultations directly from the app. This integration should also facilitate the automatic updating of patient information in the EHR system after each consultation.

b. Appointment Scheduling:

Develop a user-friendly interface for patients to schedule appointments in real-time. Implement automated reminders via SMS or email to reduce no-show rates, ensuring efficient use of healthcare professionals' time.

c. Collaborative Decision-making Tools:

Implement collaborative decision-making tools, allowing multiple healthcare professionals to participate in real-time consultations, share opinions, and collectively decide on the best course of action for complex cases.

d. Secure File Transfer:

Enable secure file transfer functionality within the real-time services platform. This feature allows healthcare professionals to securely share documents, test results, and medical images with colleagues, ensuring efficient collaboration.

e. Remote Monitoring Integration:

Integrate real-time monitoring devices (such as wearable devices and IoT sensors) into the platform. This integration allows healthcare professionals to monitor patients remotely, providing personalized care plans based on real-time health data.

f. Automated Follow-ups:

Implement automated follow-up systems that send post-consultation surveys and health reminders to patients. Analyzing patient feedback can help enhance the quality of services, and reminders can improve patient adherence to treatment plans.

g. Emergency Response Integration:

Integrate emergency response features, allowing healthcare professionals to initiate emergency protocols, alerting nearby hospitals or emergency services, and providing critical patient information in real-time during emergencies.

By incorporating these advanced features into high-quality video conferencing and real-time services, SOHS can ensure a comprehensive and technologically advanced healthcare delivery system. These enhancements not only elevate the patient experience but also optimize collaboration among healthcare professionals, leading to better healthcare outcomes and patient satisfaction.

3. Staff Access to Services from Home:

a. Secure Virtual Private Network (VPN):

Set up a secure VPN for staff to access SOHS's network remotely. VPN connections will provide encrypted tunnels, safeguarding data during transmission, and ensuring secure access to internal resources.

b. Multi-Factor Authentication (MFA):

Enforce multi-factor authentication for all staff members accessing services remotely. MFA adds an extra layer of security, requiring multiple forms of verification, such as passwords and authentication codes, ensuring authorized access.

4. Remote Desktop Services:

Implement Remote Desktop Protocol (RDP) or similar secure remote desktop services, allowing staff to securely access their workstations from home. This ensures that staff can use specialized medical software and access patient records securely.

5. Training and Support:

Provide comprehensive training sessions for staff on securely accessing and using services from home. Training should emphasize security protocols, proper data handling, and adherence to compliance standards.

- Offer 24/7 technical support to assist staff with any issues encountered while accessing services remotely, ensuring continuous and uninterrupted healthcare operations.

iii. Confidence

Service Level Agreements (SLA) for Different Services: Ensuring Seamless Healthcare Operations

In the fast-paced world of healthcare, where every second matters, the effectiveness and reliability of services provided are critical. Secure On-demand Health Services (SOHS) recognizes this importance and has established stringent Service Level Agreements (SLAs) to ensure seamless healthcare operations and patient satisfaction. These SLAs are meticulously designed to govern various aspects of service delivery, response times, issue resolution, and most importantly, data security.

Downtime:

1. Video Conferencing:

Target: No more than 0.1% downtime annually for video conferencing services.

- *Immediate Remediation:* Any downtime exceeding the stipulated limit triggers an immediate investigation. A dedicated response team works diligently to identify the root cause and swiftly remedy the situation, minimizing service disruption.

2. Real-time Services:

Target: Real-time services downtime should not exceed 0.5% annually.

- *Communication of Maintenance Activities:* Scheduled maintenance activities are communicated well in advance to all stakeholders, ensuring transparency and allowing them to plan their activities accordingly.
- *Emergency Downtimes:* In the rare event of an emergency downtime, the IT support team mobilizes promptly. Emergency downtimes are resolved within the shortest possible timeframe to restore services swiftly.

System Response Times:

1. Login Time:

Target: Users should be able to log in within 2 seconds of entering their credentials.

- *Efficiency and User Experience:* SOHS places a premium on user experience. Rapid login times ensure that healthcare professionals can swiftly access the system, maximizing their efficiency and enabling them to focus on patient care.

2. Data Retrieval:

Target: Response time for retrieving patient records should not exceed 3 seconds under normal operational load.

- *Instant Access to Patient Information:* Timely retrieval of patient records is paramount. Healthcare professionals rely on instant access to accurate patient information to make informed decisions. Meeting this SLA ensures that patient data is readily available during consultations, enabling comprehensive and personalized care.

3. Appointment Scheduling:

Target: Staff should be able to schedule appointments and confirm bookings within 5 seconds per transaction.

- *Efficient Workflow:* Efficient appointment scheduling is pivotal for managing patient flow. Meeting this SLA empowers staff to streamline their workflow, ensuring that patients are scheduled promptly and receive the necessary medical attention without unnecessary delays.

Issue Resolution:

1. Critical Issues:

Target: Critical issues impacting patient care must be resolved within 2 hours of being reported.

- *Rapid Response Team:* A specialized team is on standby to address critical issues. This team comprises experienced professionals who swiftly diagnose the problem, implement solutions, and validate the resolution to ensure seamless patient care.

2. Non-Critical Issues:

Target: Non-critical issues should be resolved within 24 hours of being reported to the IT support team.

- *Continuous Improvement:* While non-critical, these issues are nonetheless essential for optimizing the system. Timely resolution ensures that the healthcare professionals' workflow remains uninterrupted, fostering a culture of continuous improvement within SOHS.

Data Security:

1. Data Encryption:

Requirement: All data transmission must be encrypted, ensuring compliance with healthcare regulations.

- *Stringent Protocols:* SOHS employs state-of-the-art encryption protocols to safeguard patient data. Compliance with regulatory standards is non-negotiable, and any deviation from encryption protocols is treated as a severe violation of the SLA, warranting immediate corrective action.

2. Data Integrity:

Requirement: Patient data must remain intact and unaltered.

- *Vigilant Monitoring:* A dedicated team continuously monitors the integrity of patient data. Any detected discrepancies in patient records are meticulously investigated. If an inconsistency is identified, it is rectified within 4 hours of identification, ensuring the accuracy and reliability of patient information.

3. Backup and Disaster Recovery:

Requirement: Regular data backup and disaster recovery solutions must be in place to prevent data loss and ensure continuity in case of disasters.

- *Resilience in the Face of Adversity:* SOHS acknowledges the importance of data continuity. Robust backup and disaster recovery mechanisms are meticulously maintained, ensuring that even in the face of unforeseen events, patient data remains secure, and services can swiftly resume without compromising patient care.

4. Regular Security Audits:

Requirement: Regular security audits must be conducted to identify vulnerabilities and reinforce security measures.

- *Staying Ahead of Threats:* SOHS adopts a proactive approach to security. Regular security audits are conducted to identify potential vulnerabilities. Addressing these vulnerabilities promptly ensures that SOHS stays ahead of evolving cybersecurity threats, safeguarding patient data and maintaining the trust of the community.

In summary, these SLAs form the backbone of SOHS's commitment to delivering exceptional healthcare services. By adhering to these stringent agreements, SOHS not only ensures the efficiency of its operations but also upholds the trust of patients and healthcare professionals alike. The continuous monitoring, rapid response, and commitment to security and data integrity make SOHS a reliable and secure healthcare provider, dedicated to providing the best possible care to the community it serves.

4. Conclusion

The Secure On-demand Health Services (SOHS) network design is blueprint tailored to address the unique demands of delivering specialized healthcare to the community. Drawing on cutting-edge technologies like cloud services, virtualization, VPNs, QoS, load balancers, CDNs, and a suite of security measures, the design promises a blend of security, dependability, scalability, and efficiency. All the while, it remains in strict alignment with industry standards and pertinent healthcare regulations.

The network design proposed combines the best of hub-and-spoke and service-oriented architectures. Anchored at the Inner Sydney office as a hub which effectively links to three subsidiary GP practices via integrated routers and switches. Each GP unit manages different functions like central database, backup mechanisms, web servers, and a range of critical security and network management systems to ensure maximum availability. QoS measures have been strategically deployed to give precedence to vital medical data streams, including telemedicine and robotic surgical data. Furthermore, the design heavily incorporates redundancy—from backup internet connections to cloud backup services—to guarantee high uptime and resilience.

SOHS's design has followed a meticulous procedure, encompassing stages from initial analysis right through to post-implementation evaluation. This is to ensure network is strategic and is ready to evolve with shifting demands. But it is not without challenges or limitations. Some of the potential challenges include budget constraints, staff training and support needs, interoperability issues with existing healthcare IT systems or external providers, security threats from cyberattacks or natural disasters, performance issues due to congestion or latency, scalability issues due to growing demand or expansion plans, compliance issues due to evolving regulations or standards, etc. These challenges require constant monitoring and evaluation of the network performance and security posture. They also require regular updates and enhancements of the network infrastructure and components.

None the less, this network design present a starting point to build a full scale health care system which integrate the client demands. It serves as a prototype—an initial blueprint—that, while robust and forward-thinking, is ultimately a foundation. This foundation is laid with the flexibility to adapt, scale, and innovate as technology evolves and as healthcare demands shift.

5. Bibliography

Elrod, JK & Fortenberry, JL 2017, ‘The hub-and-spoke organization design: an avenue for serving patients well’, *BMC Health Services Research*, vol. 17, no. S1.

Guan, W, Wen, X, Wang, L, Lu, Z & Shen, Y 2018, ‘A Service-Oriented Deployment Policy of End-to-End Network Slicing Based on Complex Network Theory’, *IEEE Access*, vol. 6, pp. 19691-701.

McCabe, JD 2010, *Network Analysis, Architecture, and Design*.

Chapter 1 - Kizza, J. M. (2020). Computer Network Fundamentals. In J. M. Kizza (Ed.), Guide to Computer Network Security (pp. 3-40). Cham: Springer International Publishing.

Poprom, Ubonsin, et al. "The Novel ICT Strategic Model for Developing of ICT in Public Universities Based on BSC." 2005, https://core.ac.uk/download/301391118.pdf.

Reimagining guest’s experience in the Hospitality industry with Facial Recognition – Facenote. https://facenote.me/reimagining-guests-experience-in-the-hospitality-industry-with-facial-recognition/

Point-of-Care Ultrasonography | NEJM Resident 360. https://resident360.nejm.org/content-items/point-of-care-ultrasonography-4

Home | Walcott Consulting. https://www.walcott.com/

Outpatient Surgery At Lee Memorial Hospital – excel-medical.com. https://www.excel-medical.com/outpatient-surgery-at-lee-memorial-hospital/

El-Gendy, M. A., Bose, A., & Shin, K. G. (2003). Evolution of the Internet QoS and support for soft real-time applications. Proceedings of the IEEE, 91(7), 1086-1104.

Lu, Y., Zhao, Y., Kuipers, F., & Van Mieghem, P. (2010). Measurement study of multi-party video conferencing. In NETWORKING 2010: 9th International IFIP TC 6 Networking Conference, Chennai, India, May 11-15, 2010. Proceedings 9 (pp. 96-108). Springer Berlin Heidelberg

Casas, P., & Schatz, R. (2014). Quality of experience in cloud services: Survey and measurements. Computer Networks, 68, 149-165.

Bethell Ltd | iManage Performance. https://imanageperformance.com/case-studies/bethell-ltd/

Safeguarding Your Business: Effective Strategies to Protect Against Fraud | Timothy D. McGonigle, PC. https://mcgoniglelaw.com/safeguarding-your-business-effective-strategies-to-protect-against-fraud/

Transitioning to Hosted Desktop Services: Tips for a Smooth Migration - Green Poison. https://greenpois0n.com/hosted-desktop-services/

6. Credits

1. Analysis and Requirement Gathering

Owner: Nishat Sharmila

ID: 8221819

Responsibility: Analysing the given case study in detail, identifying requirements from the interview, and gathering additional requirements needed.

Task:

Detail the requirements based on the case study and interview.
Validate the requirements with the group.

2. Network Architecture and Design

Owner: Karan Goel

ID: 7836685

Responsibility: Develop the network architecture and a first-order design for the proposed system.

Task:

Create a high-level network architecture diagram.
Identify the locations of switches, routers, and servers.
Detail any special requirements for the Inner Sydney site for the surgical robots.

3. Security and Compliance

Owner: Banin Shrestha

ID: 8447196

Responsibility: Addressing security concerns including authentication, secure connections, data encryption, and compliance with government regulations.

Task:

Propose security measures for data storage, transmission, and access.
Detail compliance requirements and how they will be met.
Develop backup and recovery strategies including cloud backup details.

4. Service Delivery and Application Requirements

Owner: Ahmed Alif Swopno

ID: 8068380

Responsibility: Ensuring that the service delivery model is robust, focusing on application requirements including high-quality video conferencing, and other specified applications.

Task:

Detail the application requirements for high-quality video conferencing and real-time services.
Address the requirements for staff access to services from home.
Detail the service level agreements (SLA) for different services, especially focusing on downtime and system response times.