Welcome

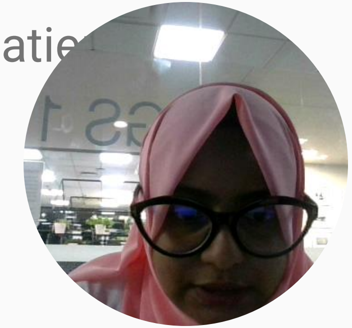
Presentation Topic: Secure On-demand Health Services (SOHS)

Group Members:

Ahmed Alif Swopno, SID: 8068380
Karan Goel , SID: 7836685,
Nishat Sharmila, SID: 8221819
Banin Sensha Shrestha, SID: 8447196

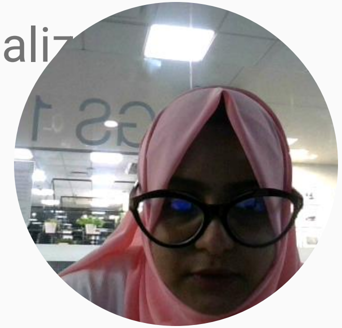
Analysis and Requirements

- Innovative Healthcare Paradigm: SOHS represents a paradigm shift in healthcare delivery, embracing a multidisciplinary approach.
- Patient-Centric Focus: Driven by rising standards, SOHS places patients' needs at the core, fostering collaborative healthcare solutions.
- Collaborative Healthcare Professionals: SOHS integrates diverse healthcare professionals, breaking traditional silos for holistic patie



Analysis and Requirements: Empowering Communities and Ensuring Security

- Community Empowerment: SOHS empowers communities by tailoring healthcare services, ensuring accessibility regardless of location or socio-economic status.
- Security and Trust: Robust security measures guarantee patient data confidentiality, building trust and confidence among patients.
- Inclusive Healthcare: SOHS embraces inclusivity, ensuring speciali healthcare services reach every corner of the community.

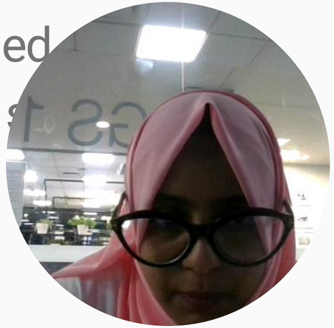


Analysis and Requirements: Futuristic Scenarios in Healthcare Delivery

- Global Telemedicine: SOHS envisions a future where telemedicine and virtual consultations transcend geographical boundaries, providing global access to specialized healthcare.
- AI and Predictive Analytics: Integration of AI and predictive analytics revolutionizes patient outcomes, alleviating the burden on healthcare systems.
- Preventive Healthcare: Real-time monitoring through wearable de empowers individuals, fostering a proactive approach to healthca

Analysis and Requirements: Network Development: Addressing Key Challenges

- User-Friendly Interfaces: SOHS designs intuitive interfaces, ensuring ease of use, especially for individuals with limited technical knowledge.
- Geographical Connectivity: VPN technology and cloud-based services overcome geographical barriers, ensuring seamless connectivity and collaboration.
- Centralized Management: Centralized management for specialized services like imaging and pathology ensures efficiency and data s



Analysis and Requirements: Comprehensive Network Design: Looking Ahead

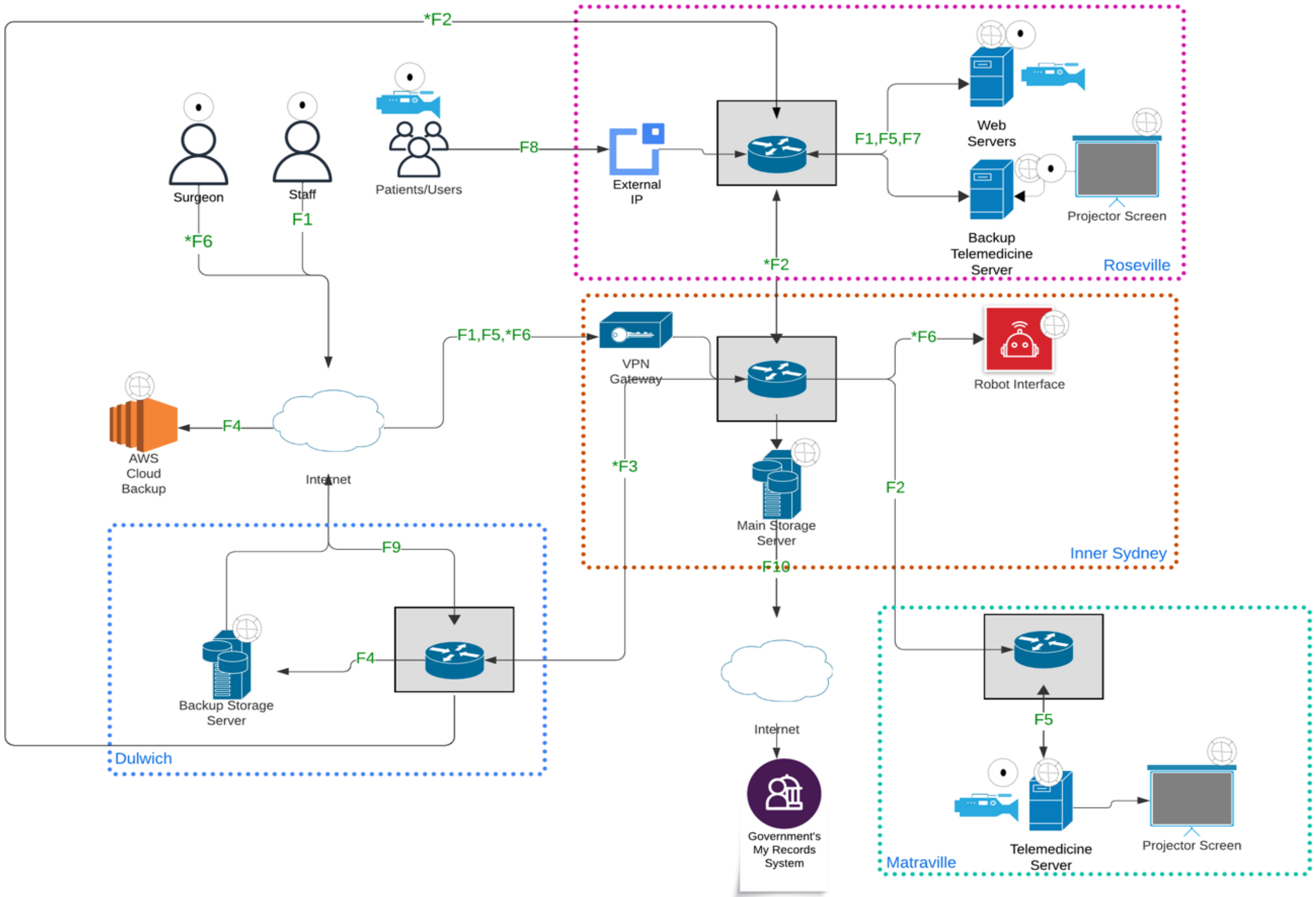
- Holistic Approach: SOHS considers scalability, redundancy, quality of service, compliance, training, interoperability, data backup, secure remote access, monitoring, and budget constraints.
- Future-Proof Network: Embracing industry best practices, SOHS creates a future-proof network capable of evolving with the dynamic healthcare landscape.
- Accessible Healthcare: The network becomes a gateway to high-
secure, and accessible healthcare for our community, aligning wi
mission.

Flow Analysis

- Flows: Sets of network traffic that have common attributes, such as source, destination, type, direction and end-to-end information

- Flow Models: Groups of flows that exhibit specific, consistent behaviour characteristics, such as directionality, hierarchy and interconnectivity.

- Flow Prioritization: Ranking of flows based on their importance, using cri as business objectives, performance requirements, security requirement number of users.



SOHS Flow Diagram

10 FLOWS OF SOHS NETWORK

1. **Staff Remote Access to SOHS Services (F1)**: This allows staff to access the internal network securely from remote locations via a VPN Gateway.
2. **Inter-office Communication (*F2)**: This critical flow enables sharing of patient records and administrative communication between different GP offices.
3. **Accessing Patient Records (*F3)**: Another critical flow, it allows any GP office to retrieve and update patient records from the Inner Sydney Database Server.
4. **Backup Processes (F4)**: This involves regular backup of patient data from the Inner Sydney Database Server to a Backup Server in another office or a Cloud Backup Service for redundancy and disaster recovery.
5. **Telemedicine Consultation (F5)**: This flow enables HD quality video consultations from patient locations to the Telemedicine Server in the respective GP office.
6. **Interactive Surgical Robots Operation (*F6)**: A critical flow that allows remote surgeons to perform surgeries with real-time controls and feedback via a VPN Gateway and the Inner Sydney Site's Robot Interface.
7. **Web-Based Services for Staff (F7)**: This flow allows staff to access personal emails, social media, etc., without compromising the integrity and security of the internal network.
8. **Public Access to SOHS Web Services (F8)**: This allows patients to access services, book consultations, view r via the public internet.
9. **Communication with Backup Cloud (*F9)**: This flow involves storing encrypted backups in a cloud service additional layer of data redundancy.
10. **Communication with Government's My Records Initiative (F10)**: This flow is for complying with gover patient data availability.

Reference Architecture

- Architectural models
- Addressing and Routing
- Network Management Architecture
- Performance Architecture
- Security and Privacy Plan

Architectural models

1. Hub and Spoke/ Star Model

Structure: Central location (hub) connects to other sites (spokes). Spokes do not connect with each other.

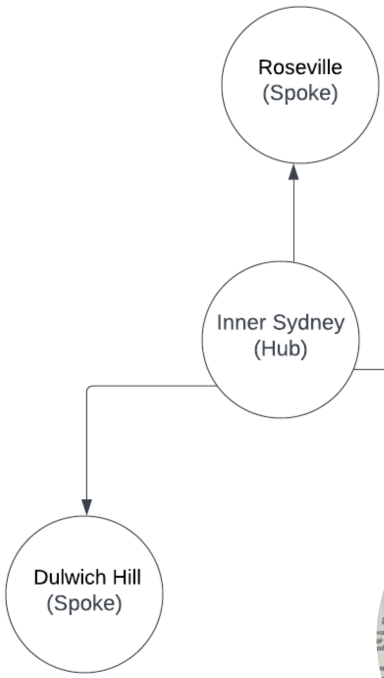
SOHS's main office in Inner Sydney is the hub.

Advantages:

- Efficiency: Streamlined paths make network monitoring and management easier.
- Centralization: Centralized services lead to cost savings and operational efficiency.

Disadvantages:

- Single Point of Failure: Vulnerable to hub failures causing all spokes to lose connectivity.
- Potential Congestion: Risk of congestion at the hub during peak times.



Hub and Spoke

Architectural models

2. Service-Oriented Model

Network design prioritizes services offered over physical locations.

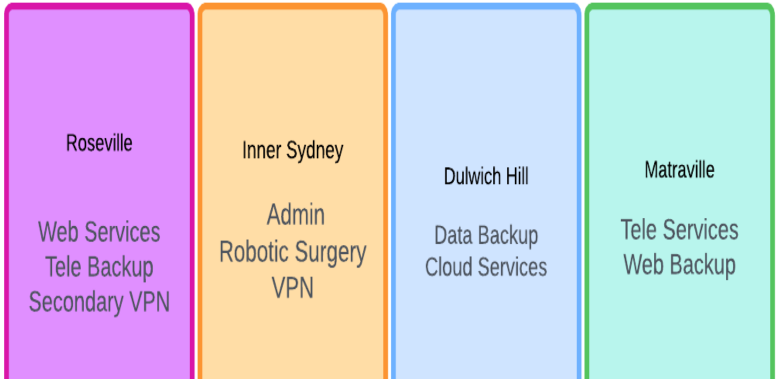
For SOHS, network divided into zones like Telemedicine, Surgical Robots, etc.

Advantages:

- Specialized Service Delivery: Tailored for smooth delivery of specialized services.
- Enhanced Security: Service-specific policies boost security.

Disadvantages:

- Resource Intensive: Might need more hardware and management resources.
- Inter-Service Communication: Risk of creating bottlenecks or inefficient paths.



Service Model Based Breakdown of Netw

Architectural models

3. Mesh Model

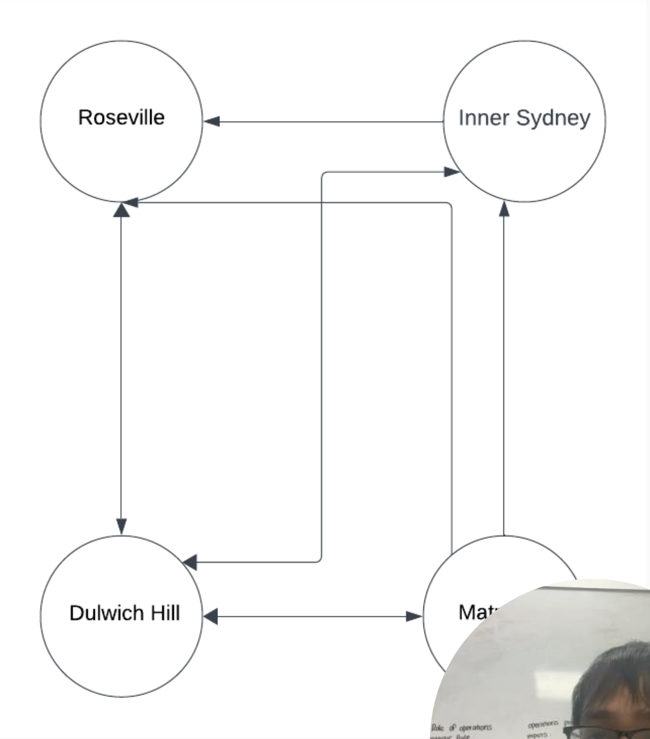
Every site interconnected to all other sites providing redundancy.

Advantages:

- High Redundancy: Alternative paths for data transfer if one link fails.
- Fault Tolerance: High due to multiple connections.
- Better Load Balancing: Traffic can be routed efficiently.

Disadvantages:

- Complex & Expensive: Due to numerous connections.
- Challenging Management: Especially as the network grows.
- Potential Congestion: Risk of congestion at the hub during peak times.



Mesh

Best - Hybrid models

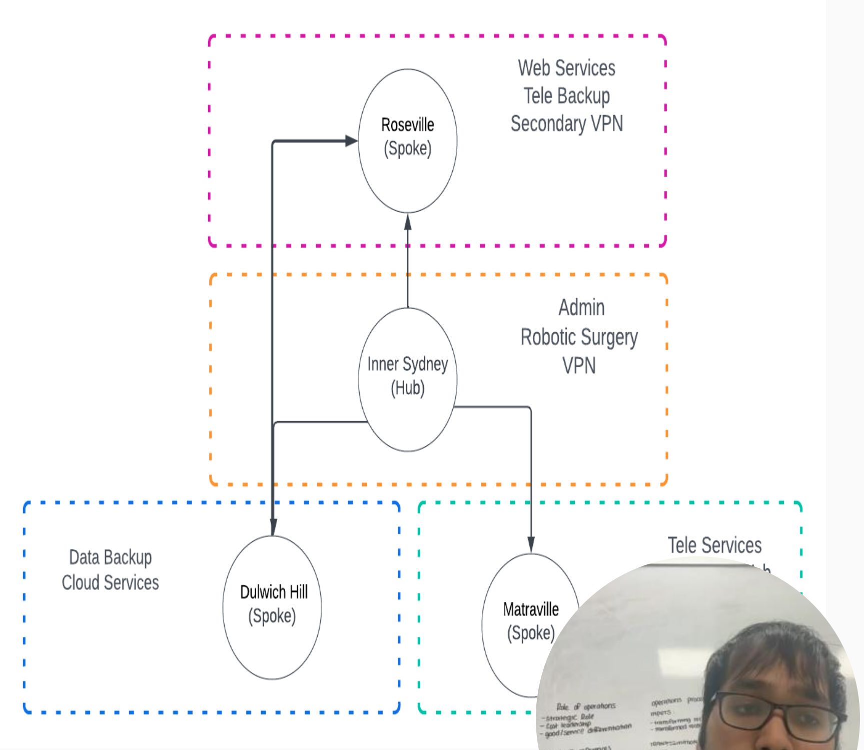
3. Hybrid Model

Combination of Hub and Spoke and Mesh Model.

Primary traffic via Hub and Spoke. Mesh between key sites for redundancy.

Advantages:

- Low Redundancy: Use backups for uptime transfer if main hub fails.
- Efficient use of resources.
- Redundancy and fault tolerance ensured,
- Inner Sydney office acts as the hub with key sites interconnected in mesh for critical services.



Hybrid of Hub/Spoke, Servic

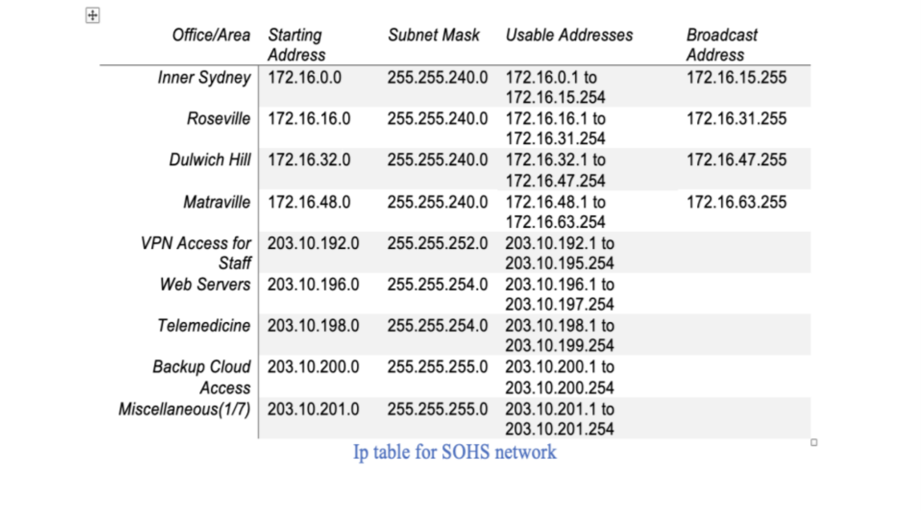
Addressing and Routing

- **Subnetting:** Creating multiple IP subnets for internal external use.
- **Routing:** Using Routing Protocols (OSPF & EIGRP).

Subnetting

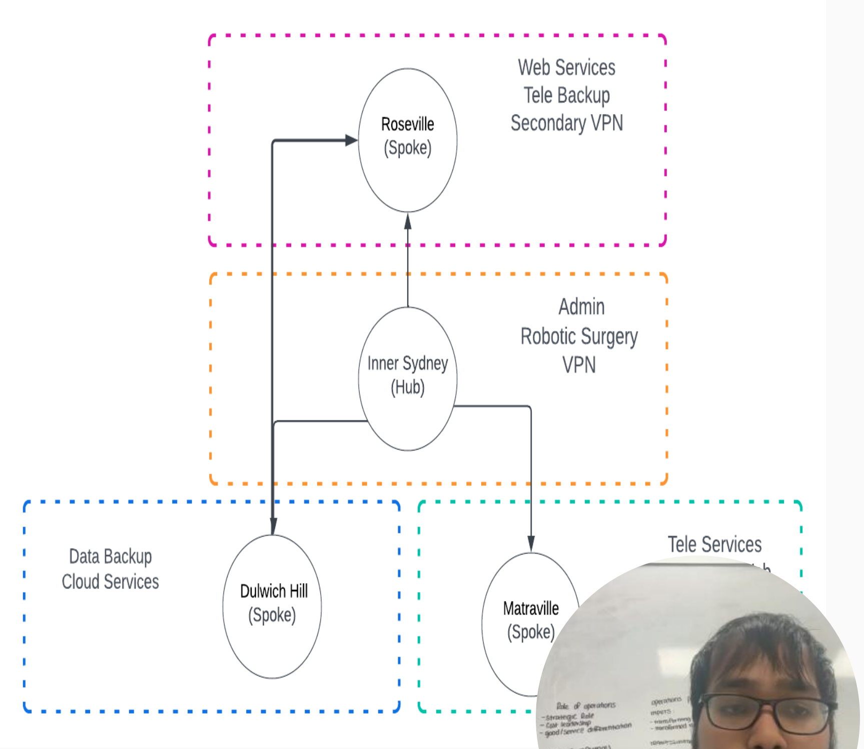
The Internal IP range 172.16.0.0/12 (1048574 add) and External IP

range 203.10.192.0/20 (4096 add) can be divided into subnets zone. The IP are divided based on requirement and location



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



IP divided based on Loca

Routing Protocols

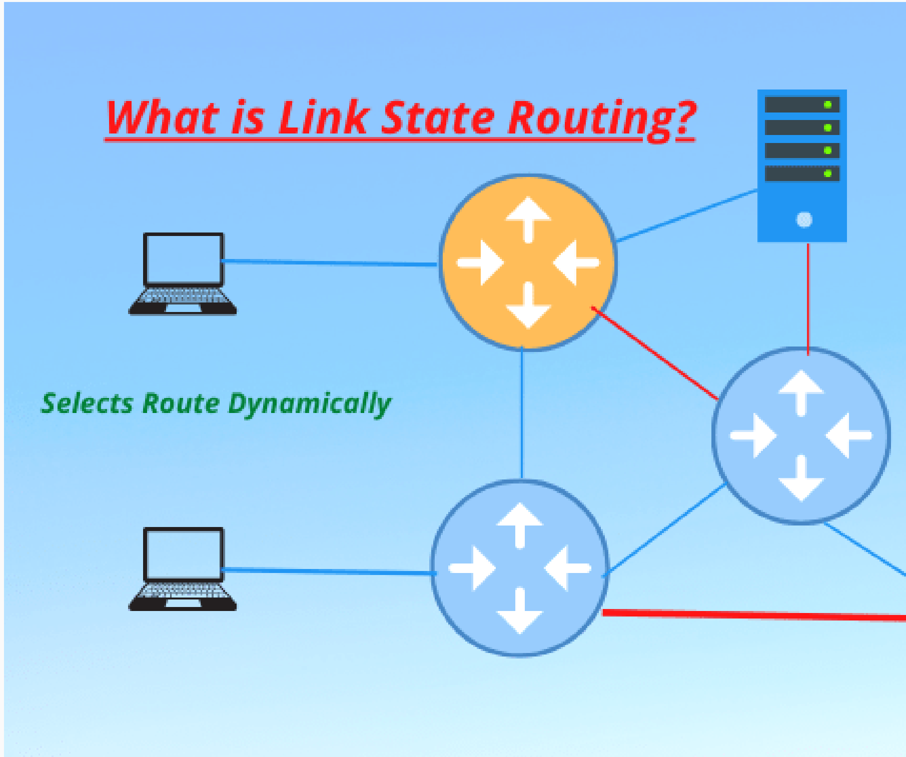
1. OSPF (Open Shortest Path First)

Link-state routing protocol using the state of links for routing decisions.

Advantages:

- Fast convergence during topology changes.
- Supports equal-cost path load balancing.

Usage in SOHS: Ensures efficient routing between main office and GP practices. Leveraged for load balancing during peak times.



2. EIGRP (Enhanced Interior Gateway Routing Protocol)

Cisco proprietary protocol combining distance-vector and link-state characteristics.

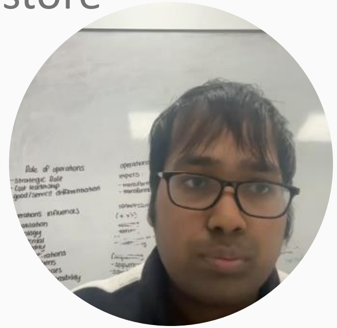
Advantages:

- Faster convergence due to Diffusing Update Algorithm (DUAL).
- Supports unequal path load balancing.

Usage in SOHS: Suitable if network is primarily Cisco. Helps route traffic considering different path metrics between GP practices and central office.

Performance Architecture

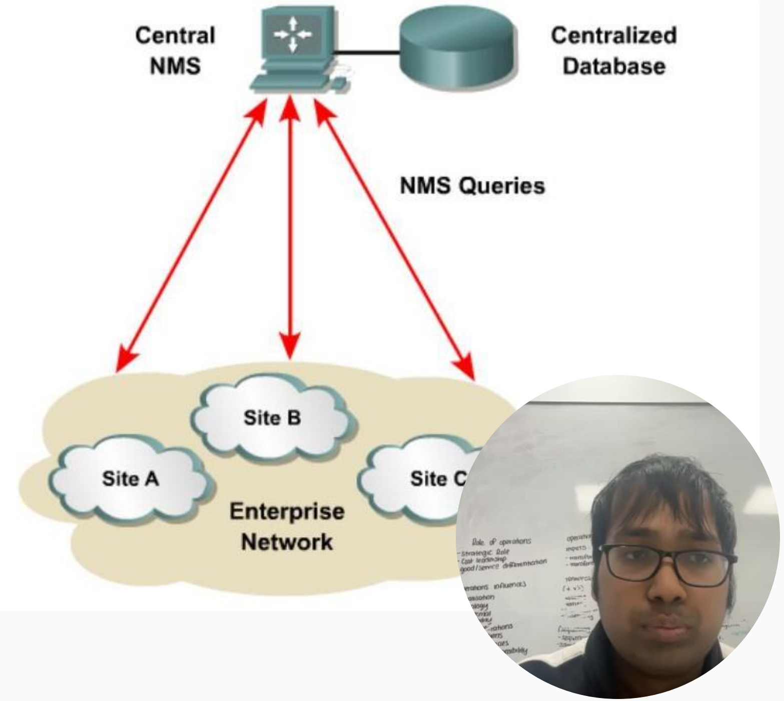
- **Quality of Service (QoS):** Mechanisms that prioritize network traffic for better performance based on predefined criteria.
- **Load Balancers:** Tools that distribute network traffic evenly across servers.
- **Redundant Links:** Backup pathways for data to ensure service continuity.
- **Content Delivery Network (CDN):** Networks of distributed servers that store cached web content.



Network Management Architecture

- **Located at Sydney**
- **Centralized Network Management:** Centralized network management consolidates all network management tools and applications in a single location

- **Remote Monitoring (RMON):** RMON is a standard monitoring specification that enables remote network monitoring of networked devices



Security and Privacy Plan

- **Security Threat Landscape:** Malware, Common Attacks, DoS
- **Security Measures:** Firewalls, Site to Site VPN, SSH

Malware

- Malware is malicious software, including:
- **Viruses:** software which inserts itself into other software and can spread from computer to computer. Requires human action to spread.
- **Worms:** a self-propagating virus that can replicate itself
- **Trojan horses:** malicious software which looks legitimate to trick humans into triggering it. Often installs back doors.
- **Ransomware:** Encrypts data with attacker’s key and asks t ransom to obtain the key.

Common Attacks

Reconnaissance

- Reconnaissance obtains information about the intended victim.
- In a targeted attack, the attacker will typically start with completely unobtrusive/non-conspicuous methods, such as searching whois information, phone directory, job listing etc.
- They will then dig deeper using tools such as ping sweeps, port and vulnerability scanners.

Social Engineering

- Social Engineering is the use of deception to manipulate individuals into providing confidential or personal information.
- It typically involves nothing more technical than the use of a telephone or email.
- The attacker will often pretend to be somebody else to trick the victim.
- Phishing is a Social Engineering attack where the attacker pretends to be from reputable company to get individuals sensitive infor

DoS (Denial of Service)

- A DoS attack prevents legitimate users from accessing an IT resource.
- It is typically a brute force style of attack which floods the target system with more traffic than it can handle.
- DoS attacks from a single source can be easily stopped by blocking traffic from the host.
- A Distributed DoS is a DoS attack from multiple sources.
- The attacker builds and controls a botnet army of infected
- A botnet is build through malware such as worms and troj

IDS and IPS

- IDS: Intrusion Detection System
- IPS: Intrusion Prevention System
- IDS and IPS use signatures to inspect packet up to layer 7 of the OSI stack, looking for traffic patterns which match known attacks.
- They can look for unusual behavior such as host sending more traffic than usual.
- IDS sits alongside the traffic flow and informs security adr potential concerns
- IPS sites inline with traffic flow and also block attacks

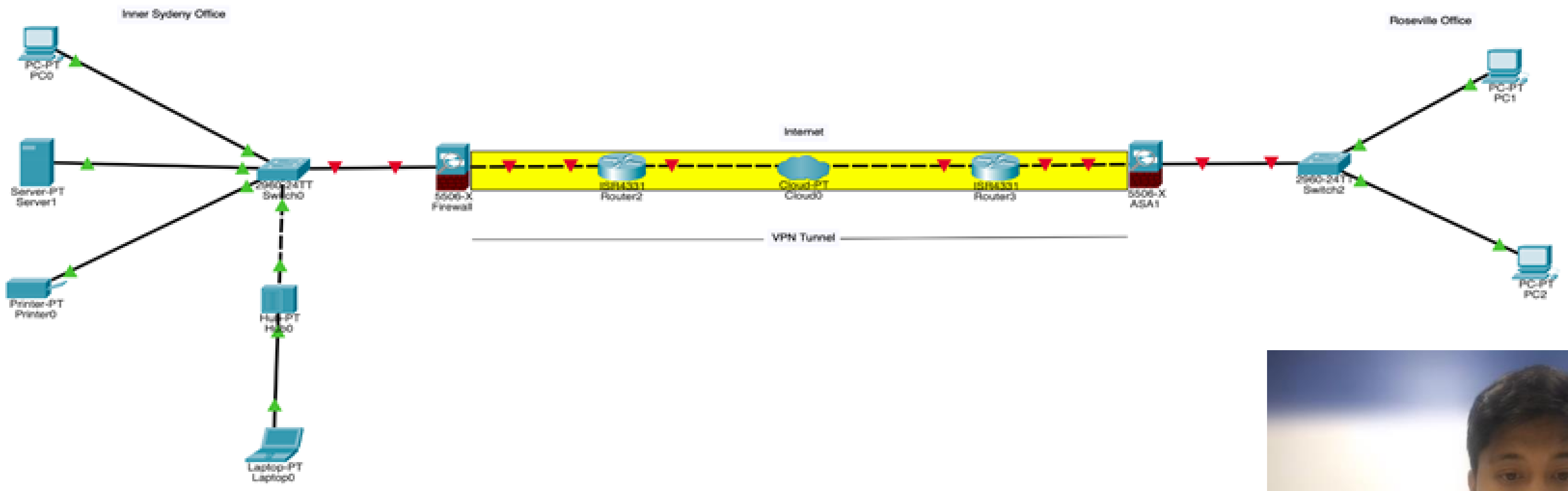
IPS vs Firewalls

- Organizations always deploy firewalls on the Internet edge. They may also deploy them at suitable security points inside their internal network.
- The line have blurred in recent years between IPS and Firewalls.
- Modern firewalls often also have IPS capability.
- They are also often capable of acting as the endpoint of VPN tunnels.

Cryptography

- Cryptography transforms readable messages into an encrypted form and then later reverses the process.
- It can be used to send sensitive data securely over an untrusted network.
- It uses authentication and encryption methods.
- **Symmetric Encryption:** the same shared key both encrypts and decrypts the data. Shared key must be kept secret.
- **Asymmetric Encryption:** uses private and public key pairs

Site-to-Site VPNs



Site-to-Site VPNs

- Site-to-Site VPNs are used when traffic needs to be sent to different location over untrusted network i.e. between two offices located in different location.
- Traffic inside an office is often unencrypted as it is seen as a trusted network
- VPN tunnels however can also be deployed internally
- Site-to-Site VPN tunnels typically terminate on a firewall o sides.

Network Device Security

- Minimal password security can be configured at three different levels.
  - **Console line:** accessing User Exec mode when connecting via console cable
  - **Virtual terminal VTY line :** accessing User Exec mode when connecting remotely via Telnet or SSH Secure Shell
  - **Privileged Exec Mode:** entering the “enable” command
- Only one administrator can connect over a console cable at a time so the line number is always 0.

Telnet vs SSH

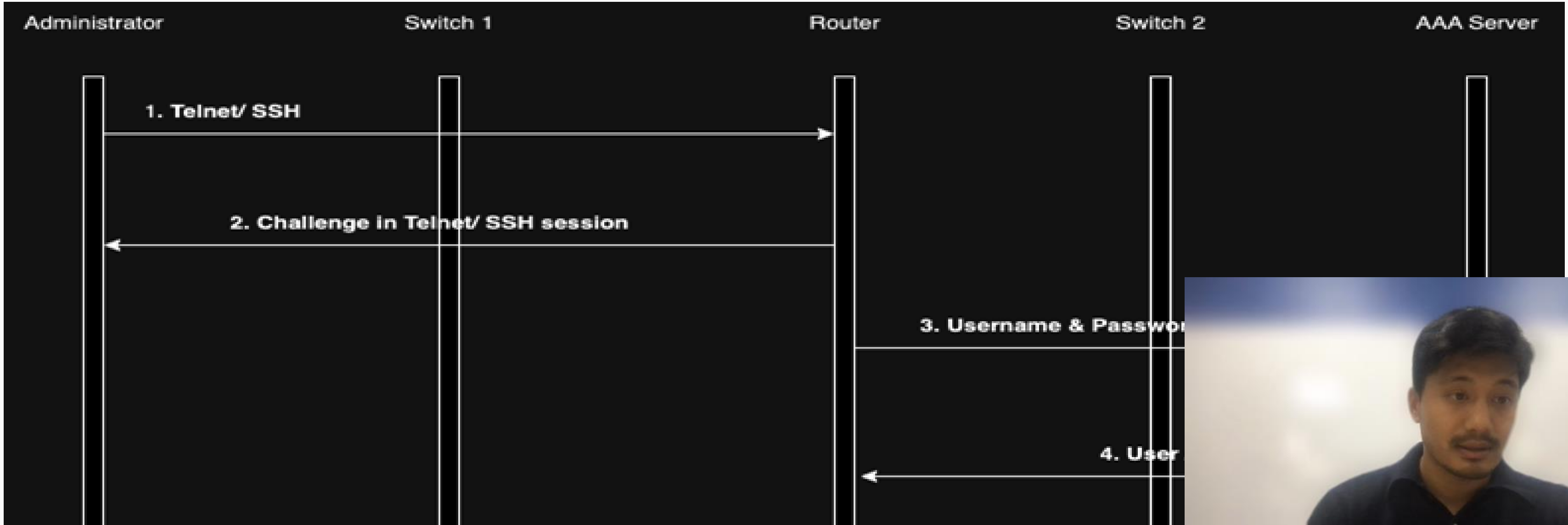
- All Telnet communications cross the network in plain text.
- If somebody sniffs the traffic using a tool such as Wireshark they can see all the commands you enter including your username and password
- All SSH Secure Shell traffic is encrypted.
- If somebody sniffs the traffic they cannot read it

AAA

- **Authentication:** verifies if somebody is who they claim they are.
- **Authorization:** level of access given to each administrator.
- **Accounting:** maintains logs or all the commands executed by the administrator.
- **Limitation of Line Level Security:**
  - Configuring line level security or local usernames on each devices has scalability limitations.
  - If password has to be added, changed or removed, it needs to be dor

How AAA works

- Sequence diagram.



Network Design

- Network Topology

1. Physical Topology
2. Logical Topology

- Design Traceability & Requirements

1. Requirements vs. Design Elements and Key Metrics
2. Design Metrics

Network Topology

Connections:

- Central hub represented by main office in Inner Sydney.

- Spokes from hub lead to various GP practices.

- Each GP practice has switches, Wi-Fi access points, and potential local servers.

- Routers from each site linked via fiber optic connections.

– VPN connections from remote workers to VPN Server in Inner Sydney.

- Secure link from Dulwich Hill Backup Server to Cloud Backup.

Locations & Components:

Inner Sydney:

- Firewall, Core router & switch, Primary database server with patient records.

- Surgical robots.

Roseville, Dulwich Hill, Matraville:

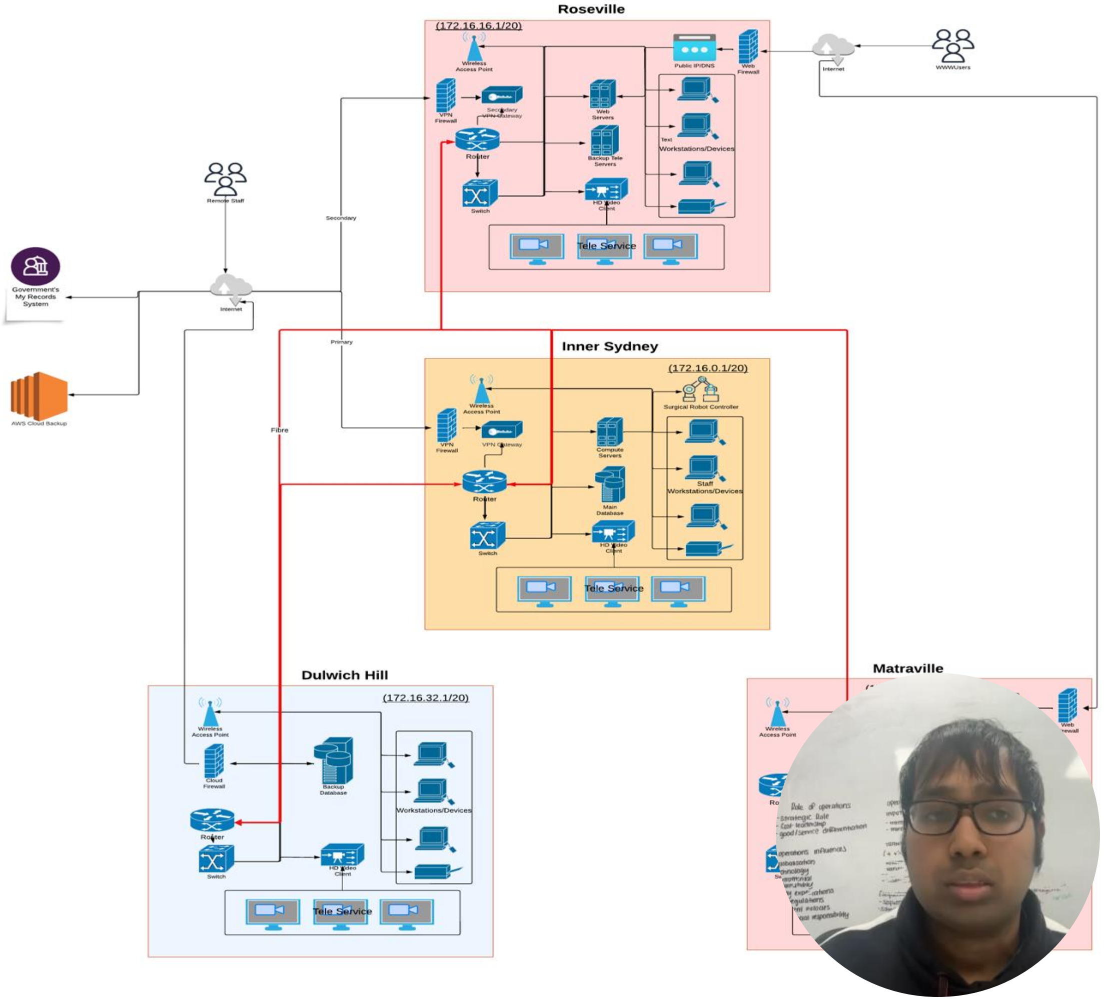
- Firewalls, routers, and switches at each site.

- DB Backup Server at Dulwich Hill.

- Secondary Web at Matraville

Cloud:

- Encrypted patient data in AWS Australian data center.



Network Topology

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.

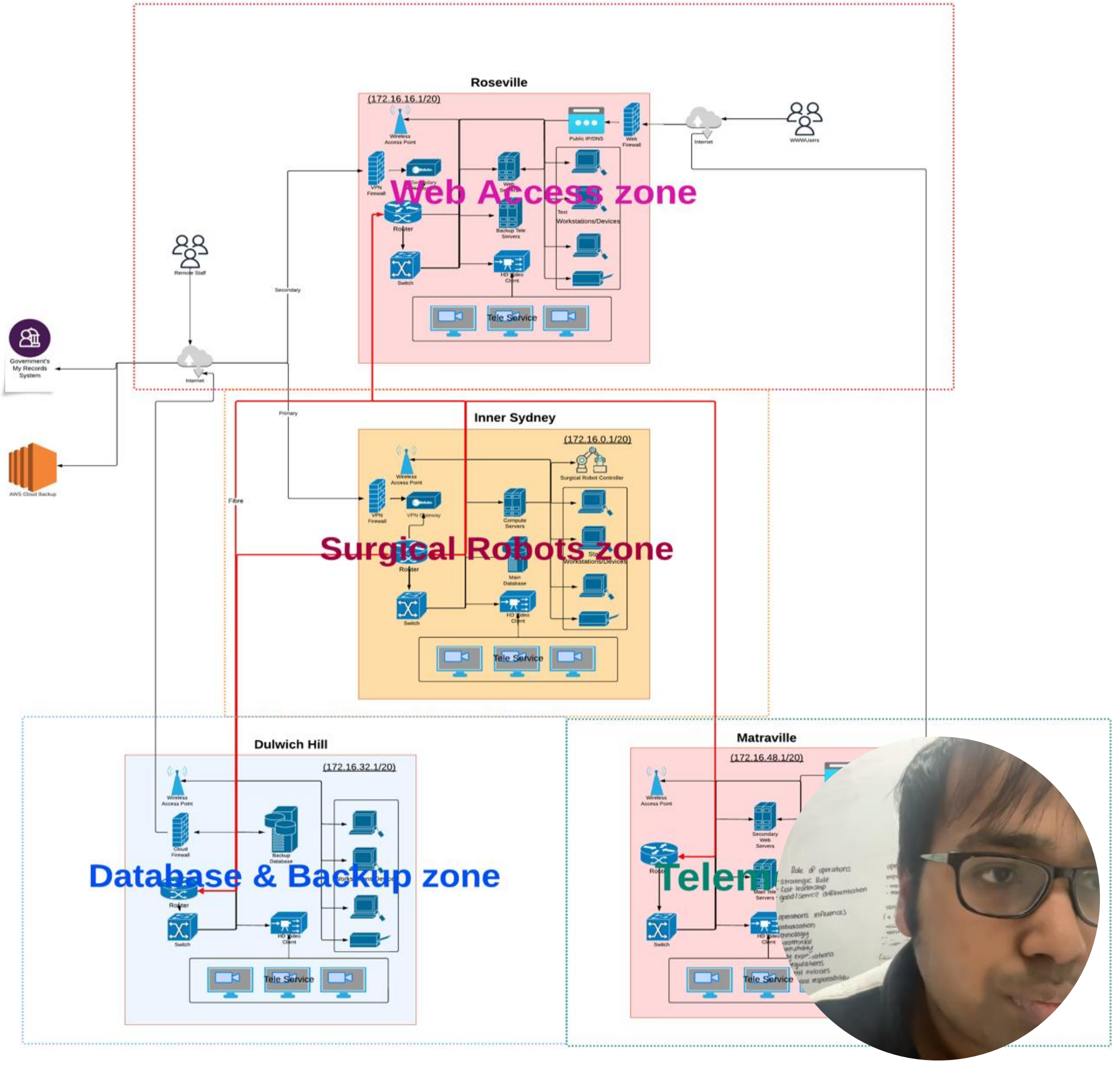
3. **Database & Backup zone**:

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.



Design Traceability

Requirements vs. Design Elements and Key Metrics

1. Seamless Communication:
   - Requirement: Efficient data sharing between main office and GP practices.
   - Design: Hub and Spoke model centralizes communication for effective data management.

2. Telemedicine Efficiency:
   - Requirement: High-quality telemedicine services.
   - Design: Service-Oriented Model's telemedicine zone optimized for seamless video and audio streaming.

3. Surgical Robot Data Security:
   - Requirement: Secure and fast data transmission for surgical robots.
   - Design: Surgical robots zone offers enhanced encryption with low-latency channels.

Design Traceability

Design Metrics

- Network Uptime: Aim for 99.99% uptime to ensure uninterrupted healthcare services.
- Bandwidth Utilization: Monitor to ensure usage does not exceed 80% even during peak times.
- Latency: Keep minimal, possibly under 50ms, for real-time applications like telemedicine and robot surgeries.
- Security Incidents: Employ advanced detection systems to track breaches, aiming for zero security incidents.
- Service Availability: Ensure critical services like telemedicine have a 99.95% availability rate, with regular audits to ensure consistency.

Lifecycle: Ensuring a Robust Service Delivery Model for Secure On-demand Health Services (SOHS)

- Comprehensive Needs Analysis: Understanding specific requirements of healthcare professionals and patients.
- Thoughtful Technology Selection: Careful evaluation of video quality, encryption, compatibility, and scalability.
- Robust Network Infrastructure: Investment in high-speed internet, QoS mechanisms, and redundancy.
- User-Friendly Interfaces: Intuitive designs for seamless interaction, focusing on user experience.

Advanced Features in High-Quality Video Conferencing and Real-time Services

- Adaptive Streaming: Adjust video quality based on internet speeds for uninterrupted service.
- Background Noise Reduction: Enhance audio clarity by eliminating background noise during consultations.
- Virtual Waiting Rooms: Secure waiting areas with status notifications for patient comfort.
- Language Support and Session Recording: Language options and session recordings for reference.

Stringent Service Level Agreements (SLAs) for Seamless Healthcare Operations

- Downtime Targets: Ensuring minimal downtime for critical services through proactive investigations.
- System Response Times: Rapid logins, quick data retrieval, and efficient appointment scheduling enhance user experience.
- Issue Resolution: Swift resolution of critical and non-critical issues fosters continuous improvement.
- Data Security Measures: Encryption, data integrity, backup, and re security audits ensure compliance and trust.

Building a Foundation for the Future: Challenges and Adaptability

- Challenges Faced: Budget constraints, staff training, interoperability, security threats, scalability, and compliance.
- Continuous Monitoring: Constant evaluation, updates, and enhancements to address evolving challenges.
- Adaptability: Flexible architecture ready to scale and innovate with evolving healthcare demands and technologies.

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/

The END

Thank You!