Fall 2025-2026
Course Name: Computer Networks
Course Code: CSE261

Alamein International University
Faculty of Computer Science and Engineering

# ***Advanced Enterprise Networking of a Secure Healthcare***

## **Under Supervision:** Dr/ Essam Abdellatef

| Student's Name | Student's ID | Academic Program |
|---|---|---|
| Rodaina Mohamed Mustafa | 23101892 | Computer Engineering |
| Sama Osama Gomaa | 23101571 | Computer Engineering |
| Jana Hazem Hegazi | 23101378 | Computer Science |
| Jana Mamdouh Hassan | 23101377 | Computer Science |
| Jowairya Mohamed Fahmy | 23101379 | Computer Science |
| Abdelrahman Mohamed | 23101577 | Computer Engineering |

## Overview:

This project focuses on the **design and implementation of a Secure Healthcare Information Network System** a multi-department healthcare organization operating across multiple floors within a corporate building. The organization supports a large and diverse user base, including medical staff, laboratory personnel, administrative teams, IT professionals, auditors, and external guests. In addition, the company relies on cloud computing services and VoIP communication systems, which further increase the complexity and security requirements of the network infrastructure.

The primary objective of this project is to design a **robust, highly available, and secure enterprise network** using a hierarchical network model that incorporates redundancy, segmentation, and centralized management. The proposed solution utilizes Cisco networking technologies to implement VLAN segmentation for LAN, WLAN, and VoIP traffic, secure perimeter defense using a Cisco ASA firewall, dynamic routing with OSPF, and high-availability mechanisms such as HSRP and EtherChannel. Virtualization and centralized server infrastructure are employed to enhance resource utilization, fault tolerance, and business continuity, while wireless and VoIP services are integrated to support modern communication needs.

Due to security requirements, it has been decided that all LAN, WLAN, and VoIP users will be on a separate network segment within the same local area network. The firewall will be used to set security zones and filter traffic that moves in and out of the zones based on the configured inspection policies.
You have been hired as a network security engineer to design the network according to the requirements set by the senior management. You will consult an appropriate robust network design model to meet the design requirements. You are required to design and implement a secured, reliable, scalable, and robust network system that is paramount to safeguarding the Confidentiality, Integrity, and Availability of data and communication.

By implementing industry best practices in network design and security, this project aims to deliver a scalable infrastructure capable of supporting current operational requirements while accommodating future growth. The final network solution ensures secure internal and external connectivity, efficient resource management, and reliable service delivery, making it well-suited for a healthcare environment where data protection and system availability are paramount

## Components Used:

| Name of the Component | Amount Used | Purpose in the Project |
|---|---|---|
| ISP Router (Airtel) | 1 | Provides internet connectivity and access to external networks using public IP addresses. |
| Cisco ASA 5500-X Firewall | 1 | Secures the network by filtering traffic, creating security zones, and protecting sensitive healthcare data. |
| Cisco WAN Router (Cisco 2811) | 1 | Handles routing between networks and supports VoIP telephony services. |
| Cisco Catalyst 3850 (48-Port Multilayer Switch) | 2 | Acts as core switches, enabling inter-VLAN routing, redundancy, and high-speed backbone connectivity. |
| Cisco Catalyst 2960 (48-Port Access Switch) | 8 | Connects end devices and enforces VLAN segmentation at the access layer. |
| Cisco Catalyst 2960 (24-Port Access Switch) | 2 | Provides additional access layer connectivity for departments with fewer devices. |
| HP ProLiant DL380 Gen10 Servers | 2 | Hosts virtual machines and provides redundancy and high availability for critical services. |
| VMware ESXi Hypervisor | 2 | Enables server virtualization to optimize hardware usage and support failover. |
| Red Hat Directory Server (LDAP, DNS, DHCP) | 1 (Redundant) | Manages user authentication, name resolution, and dynamic IP address allocation. |
| Health Information System Server | 1 | Stores and manages patient medical records and healthcare data securely. |
| Email Server | 1 | Provides secure internal and external email communication. |
| File Server | 1 | Enables centralized file storage, sharing, and data access control. |
| NetApp Storage Devices | 2 | Provides centralized, high-performance, and redundant data storage. |
| Cisco Voice Gateway | 1 | Enables Voice over IP (VoIP) communication and internal dialing services. |
| Wireless LAN Controller (WLC) | 1 | Centrally manages wireless access points and wireless security policies. |
| Lightweight Access Points (LAPs) | 10 | Provides wireless connectivity to staff, guests, and auditors across departments. |
| AWS Cloud Platform | 1 | Supports cloud-based services, global access, and business continuity. |
| IP Phones | Multiple (per department) | Enables VoIP communication within the organization. |
| End-User Devices (PCs/Laptops) | Multiple | Used by employees for daily clinical, administrative, and IT operations. |

## Building and End-User Device Distribution

The healthcare organization operates within a single corporate building, occupying the **35th, 36th, and 37th floors**. Each floor hosts specific departments, and each department is equipped with a defined set of end-user devices to support daily operations, communication, and network services.

## A) 35th Floor – Medical Operations and Reception Services

### I. Medical Laboratories and Pharmacy

The medical laboratories and pharmacy are located on the 35th floor. Each lab/pharmacy unit is equipped with the following devices to support clinical and pharmaceutical operations:

- 3 Desktop PCs
- 1 Network Printer
- 1 PH-LAP
- 1 IP Phone
- 1 Smartphone
- 1 Laptop
- 1 Tablet

### II. Reception and Guest Area

The reception and guest area is also located on the 35th floor and supports front-desk operations, visitor management, and guest connectivity. The area is equipped with:

- 2 Desktop PCs
- 1 Network Printer
- 1 IP Phone
- 1 PH-LAP
- 1 Tablet
- 1 Smartphone
- 1 Laptop

## B) 36th Floor – Medical Consultancy and Administrative Services

### I. Doctors’ Consultancy Department

The doctors’ consultancy department on the 36th floor supports patient consultations and clinical decision-making. Each consultancy unit is equipped with:

- 2 Desktop PCs
- 1 Network Printer
- 1 IP Phone
- 1 DOC LAP
- 1 Tablet
- 1 Smartphone
- 1 Laptop

### II. Procurement, Human Resources and Finance Department

The **Procurement**, HR and Finance department, also located on the 36th floor, supports administrative, payroll, and procurement functions. Each unit is equipped with:

- 2 Desktop PCs
- 1 Network Printer
- 1 IP Phone
- 1PRO-LAP
- 1 Laptop
- 1 Tablet
- 1 Smartphone

## C) 37th Floor – Corporate and IT Services

### I. Corporate Department

The corporate department on the 37th floor supports executive management and internal audit functions. Each corporate office is equipped with:

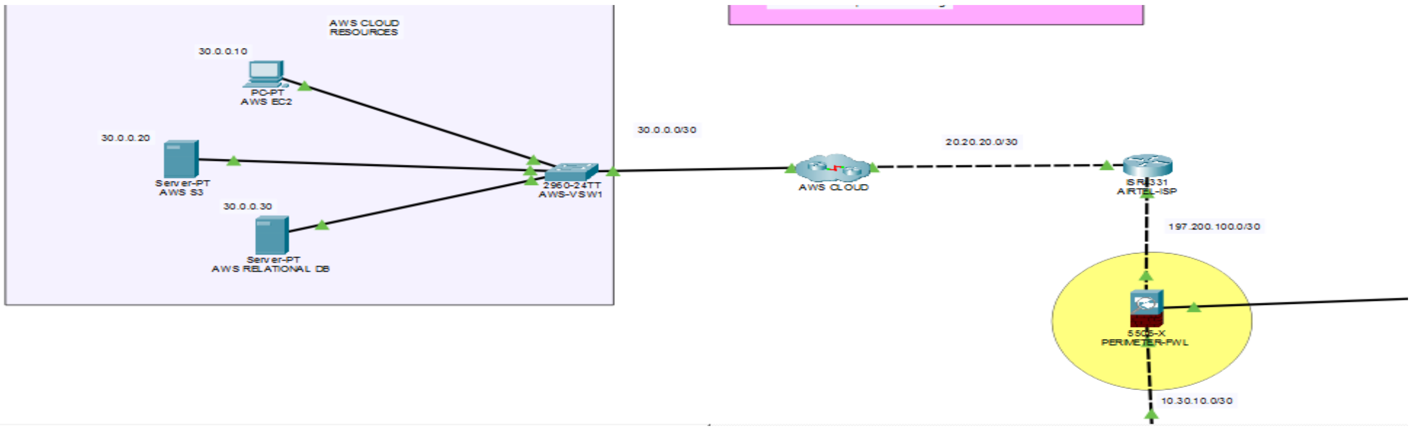
- 2 Desktop PCs
- 1 Network Printer
- 1 Phone
- 1 Tablet
- 1 Smartphone
- 1 Laptop

## II. Information Technology (IT) Department

The IT department, also located on the 37th floor, supports all technical operations, including network management, cybersecurity, system administration, software development, and cloud services. The IT team uses the same set of end-user devices as the corporate department:

- 2 Desktop PCs
- 1 Network Printer
- 1 Phone
- 1 Tablet
- 1 Smartphone
- 1 Laptop

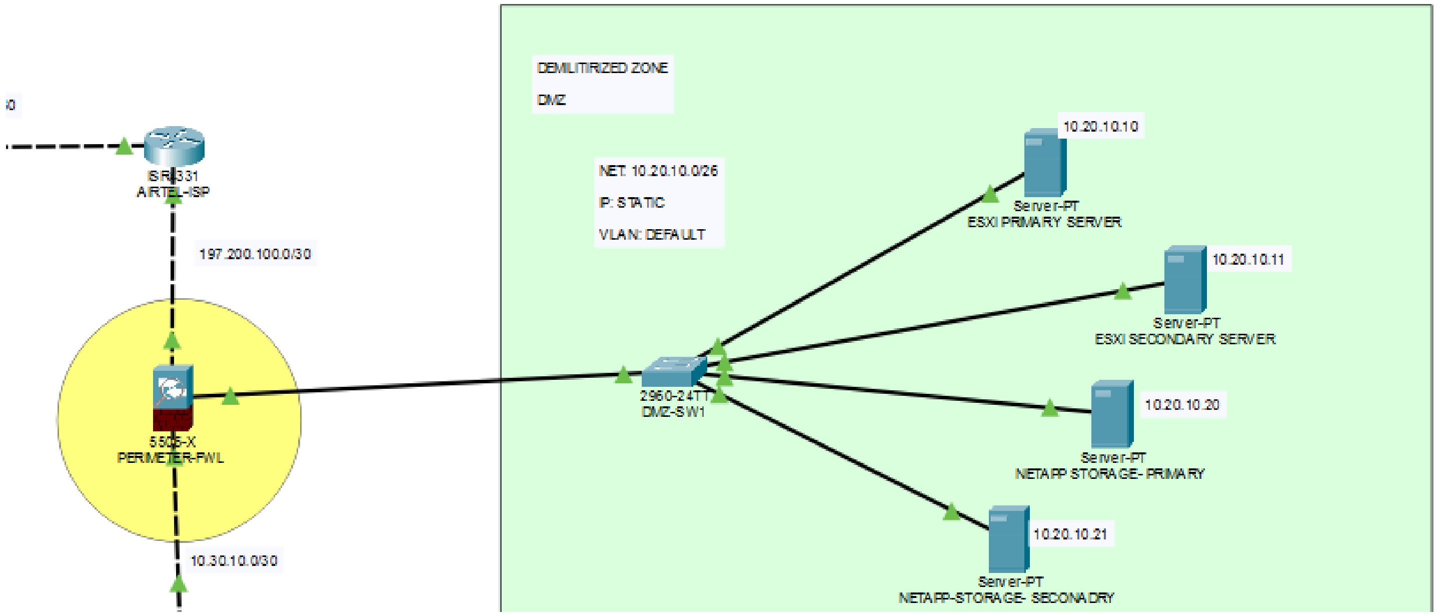
## Module-by-Module Explanation



To ensure high availability and global accessibility of healthcare services, the network infrastructure integrates a dedicated Cloud Computing segment leveraging the **AWS platform**.

This architecture facilitates the hosting of critical application workloads on **AWS EC2**, scalable data storage via **AWS S3**, and managed database services through AWS Relational DB. Secure connectivity is established through an **Airtel ISP gateway**, terminated at a **Cisco ASA 5505-X Perimeter Firewall**.

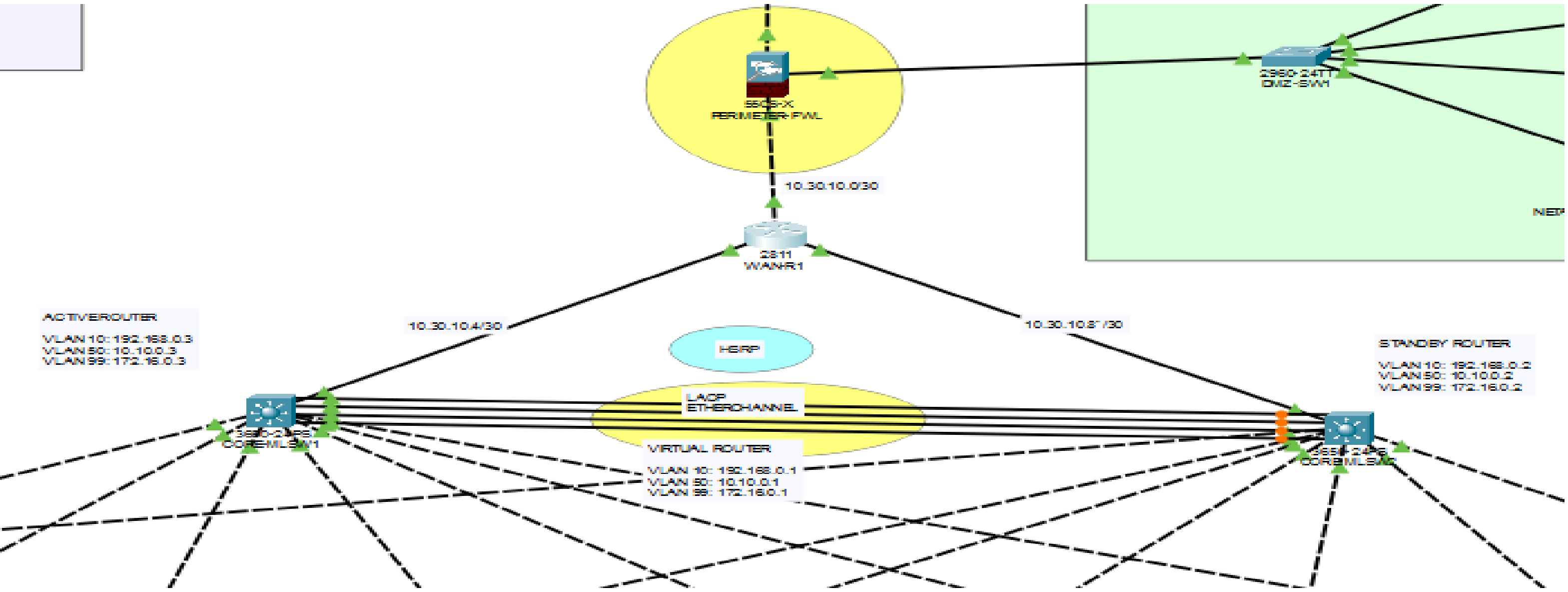
The firewall is configured with granular security policies and static routing to provide a secure tunnel for internal staff to access cloud-resident diagnostic tools while maintaining a hardened posture against external threats. This hybrid cloud approach ensures that the healthcare system remains scalable and resilient, supporting the company's projected growth and digital transformation goals.



The healthcare infrastructure implements a robust **Demilitarized Zone (DMZ)** to secure its core data assets and virtualization environment.

Utilizing **VMware ESXi on HP ProLiant hardware**, the zone provides a redundant platform for critical services, including **LDAP directory management** and **DNS**. Data integrity is further bolstered by a primary and secondary NetApp storage configuration, ensuring no single point of failure for patient records.

This segment is logically isolated by the **Cisco ASA 5505-X firewall**, which enforces strict access control policies to mitigate risks while allowing authorized external and internal service requests to be processed securely.

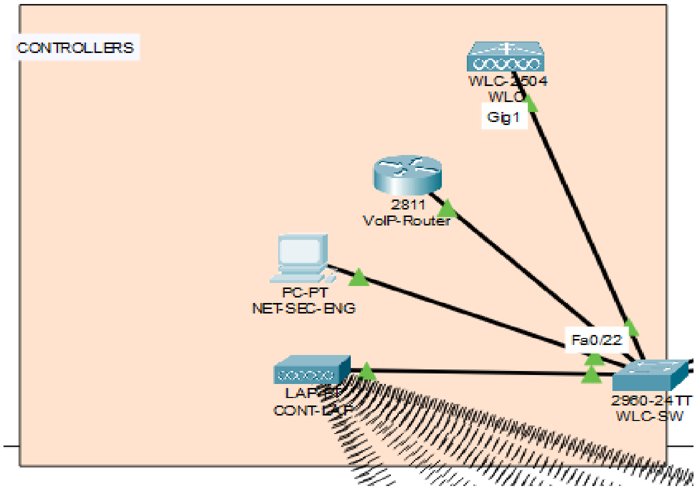


The proposed network architecture implements a robust, defense-in-depth strategy centered around a **Cisco ASA 5505-X** perimeter firewall and a high-availability core.

Internal resiliency is achieved through the integration of HSRP, providing seamless gateway failover for mission-critical **VLANs,** and **LACP EtherChannel** for optimized inter-switch bandwidth. Furthermore, the design incorporates a dedicated **Demilitarized Zone (DMZ)** on the **10.20.10.0/26 subnet** to isolate sensitive compute and storage assets, including **redundant ESXi hosts** and **NetApp storage arrays.**

This tiered approach ensures that critical healthcare data remains highly available while maintaining strict logical separation between internal user traffic, server resources, and external cloud services.

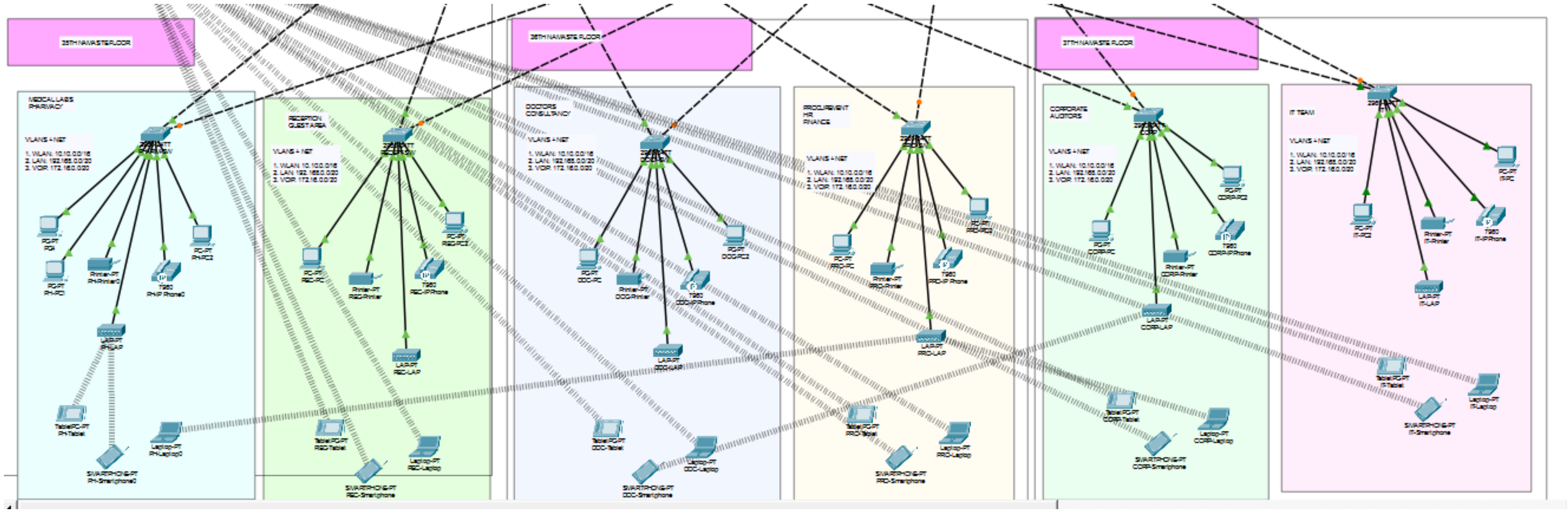
The network architecture incorporates a centralized Control and Management segment designed to streamline administration while maintaining a rigorous security posture.



At the heart of this segment is the **Cisco 2504 Wireless LAN Controller (WLC)**, which provides unified management for the **lightweight access point** infrastructure and enforces role-based **SSID segmentation.**

Telephony services are delivered via a dedicated **Cisco 2811 VoIP router,** ensuring high-quality voice communication across all clinical departments. To safeguard the management plane, the design restricts remote administrative access (**SSH**) exclusively to the Senior Network Security Engineer's terminal.

This centralized approach, aggregated through a high-performance **Catalyst 2960 switch**, ensures that critical infrastructure components remain logically isolated from general user traffic while remaining highly accessible for authorized configuration and monitoring



The distribution layer of the healthcare facility is architected across a three-floor physical topology, employing a rigorous **VLAN segmentation** strategy to isolate departmental traffic and prioritize mission-critical services.

By deploying dedicated access switches and **lightweight access points** within the Pharmacy, Clinical, and Administrative zones, the design ensures robust connectivity for both wired and wireless endpoints. Security is enforced at the port level by assigning devices to specific **VLANs—VLAN 10 for management**, **VLAN 20 for general data**, and **VLAN 99 for high-priority Voice-over-IP (VoIP) traffic.**

This hierarchical distribution model, characterized by redundant uplinks to the core infrastructure, provides the necessary scalability and fault tolerance required for a high-traffic medical environment while maintaining the confidentiality and integrity of patient information.

## Tables and Summaries

| VLAN ID | Type / Name | Usage / Purpose | Location |
|---|---|---|---|
| **VLAN 10** | **Management / WLAN** | Used for wireless infrastructure management and central administration. | Across all floors (35th, 36th, 37th) and the Controllers zone. |
| **VLAN 20** | **Data / LAN** | Primary network for wired endpoints (PCs, Laptops, Printers). | Pharmacy, Medical Labs, HR, Finance, and IT Team zones. |
| **VLAN 50** | **Administrative** | Isolated segment for sensitive corporate and auditing functions. | 36th Floor (HR/Finance) and 37th Floor (Corporate Auditors). |
| **VLAN 99** | **VoIP** | Dedicated high-priority network for IP phones to ensure voice quality. | Distributed to all departmental desks across all floors. |
| **VLAN 1** | **Default** | Standard native VLAN; used **primarily** for control traffic in the DMZ. | DMZ aggregation switch (DMZ-SW1). |

The network architecture utilizes a strategic **VLAN framework** to achieve logical segmentation and enhance the overall security posture of the healthcare facility.

By isolating clinical data in **VLAN 20**, administrative functions in **VLAN 50**, and high-priority voice traffic in **VLAN 99**, the design effectively reduces the size of broadcast domains and mitigates the risk of unauthorized lateral movement within the network. Each department is confined to its own dedicated subnet, ensuring that sensitive financial or patient information is not visible to unauthorized segments. This logical isolation is further enhanced by the use of **VLAN 10** for centralized wireless management and **VLAN** 1 as the default for control traffic.
Furthermore, every VLAN is supported by a **redundant gateway** implemented through HSRP on the core switches, which ensures that departmental connectivity remains uninterrupted even in the event of a hardware failure.

| Protocol | Type | Why We Used It (Purpose) | Where It Was Used | How It Was Applied in the Project |
|---|---|---|---|---|
| **HSRP** | Redundancy | To provide a resilient gateway for the network. | **Core Multilayer Switches** (Core-MLSW1 & Core-MLSW2). | Created a "Virtual Router" IP (e.g., 192.168.0.1) that remains active even if one switch fails. |
| **LACP** | Aggregation | To increase bandwidth and provide link failover. | **Between Core Switches**. | Bundled multiple physical cables into a single high-speed "EtherChannel" logical link. |
| **OSPF** | Routing | To dynamically share network paths. | **Firewall, Routers, and Core Switches**. | Configured to advertise routes so internal users can reach the DMZ and AWS Cloud resources. |
| **DHCP** | Addressing | To automate IP assignment for end-devices. | **Red Hat Directory Server** in the DMZ. | Configured to dynamically assign IP addresses to PCs, laptops, and tablets throughout the floors. |
| **SSH** | Security | To encrypt remote management sessions. | **All Routers and Switches**. | Restricted access exclusively to the **Senior Network Security Engineer's PC**. |
| **802.1Q** | Trunking | To carry traffic for multiple VLANs over one link. | **Trunk Links** between Access and Core Switches. | Tagged frames to maintain departmental isolation as data moves across the network backbone. |
| **CUCME** | Voice | To manage the internal phone system. | **2811 VoIP-Router**. | Managed directory numbers (3000-3020) and provided dial tones to all IP phones. |

## Conclusion

In conclusion, the implementation of this healthcare network infrastructure establishes a highly resilient, secure, and scalable foundation tailored to the demanding requirements of a modern medical facility.

By integrating a multi-layered defense-in-depth strategy, the design successfully balances high-speed performance with stringent data protection protocols. The core of the network, fortified by redundant multilayer switches and protocols such as **HSRP** and **LACP EtherChannel**, ensures near-zero downtime for critical clinical operations and department-wide connectivity.

Logical segmentation through a robust **VLAN framework**, specifically isolating clinical data, administrative management, and VoIP services, minimizes the attack surface and optimizes internal traffic flow.

Furthermore, the strategic placement of a dedicated **Demilitarized Zone (DMZ)** for redundant **ESXi virtualization** and **NetApp** storage arrays ensures that sensitive patient records and server resources remain highly available yet isolated from external threats by the **Cisco ASA perimeter firewall**. The inclusion of centralized wireless management via a **WLC** and prioritized telephony services through **CUCM**E provides a seamless communication experience for staff across all floors.

Ultimately, this architecture not only meets current operational demands but also provides a future-proofed environment capable of evolving with emerging healthcare technologies and regulatory compliance standards.