AlShifa Hospital Comprehensive Network Infrastructure

NAME
Sherif thabit ahmed jacoub
Mahmoud Al sayed shreef

Designed and Configured by: Sherif Thabit Ahmed Jacoub (Team Leader & Troubleshooting)

Help Desk Support: Mahmoud Al Sayed Shreef

Table Of Contents

Abstract

The **Al-Shifa Hospital Network Infrastructure** project is designed to provide **Al-Shifa Hospital** with a resilient, secure, and scalable network that connects its main hospital building seamlessly. Addressing the critical needs of a modern healthcare institution, this initiative focuses on creating a network that supports high-performance connectivity, data protection, and compliance with stringent healthcare regulations. By implementing a sophisticated design, the project ensures secure, efficient communication across all departments, meeting the operational demands of today's highly regulated healthcare environment.

The project scope includes both physical and logical network layers, integrating advanced technologies that provide a multi-layered approach to security and network management. Core elements include VLAN segmentation, access controls, and centralized management protocols, which together fortify the network against unauthorized access and potential data breaches. The redundancy and failover configurations ensure that the network remains highly available and resilient, maintaining service continuity even in the face of hardware or connectivity disruptions.

In addition to its robust security and reliability features, the infrastructure is designed with scalability at its core. Modular network components and flexible configurations allow **Al-Shifa Hospital** to expand and adapt the infrastructure as its operations

grow and technology needs evolve. Through this approach, the network offers a future-proofed solution that supports long-term growth, positioning the hospital to confidently navigate the changing technological landscape while ensuring operational efficiency and data security.

Chapter I: INTRODUCTION

1.1 Preamble:

The **Al-Shifa Hospital Network Infrastructure** project represents a strategic initiative by **Al-Shifa Hospital** to establish a modern, secure, and interconnected network infrastructure across its main hospital location. Designed to meet the demands of a highly regulated healthcare environment, this project aims to support operational efficiency, compliance, and data protection while facilitating seamless connectivity and communication. By deploying this advanced network infrastructure, **Al-Shifa Hospital** is positioned to enhance its technological foundation, ensuring resilience, security, and scalability for years to come.

1.2 Background of the problem:

In today's digital age, healthcare institutions like **Al-Shifa Hospital** face increasing pressure to ensure data security, regulatory compliance, and reliable communication across all departments. Without an existing robust infrastructure, the hospital encounters limitations in securing sensitive patient data, achieving efficient inter-departmental communication, and adhering to compliance standards. As a response, **Al-Shifa Hospital** has chosen to implement an entirely new network infrastructure rather than upgrade an outdated system. This approach allows the hospital to maintain full control over its network design, scalability, and security measures, providing a future-ready foundation that supports growth and innovation.

1.3 Statement of the Problem:

Al-Shifa Hospital requires a secure, scalable, and highly available network infrastructure that addresses critical challenges in security, operational efficiency, and compliance. This project aims to meet these needs by implementing a state-of-

the-art network that supports high-performance connectivity between departments, secures sensitive patient data from internal and external threats, and aligns with industry regulations. Through this infrastructure, the hospital seeks to ensure continuous, reliable service, supporting seamless operations across all departments.

1.4 Objectives:

The main objectives of the **Al-Shifa Hospital Network Infrastructure** project are as follows:

- Enhance security to protect sensitive healthcare data and ensure compliance with healthcare regulations.
- Improve inter-departmental connectivity to facilitate seamless and efficient operations.
- Develop a scalable infrastructure to accommodate **Al-Shifa Hospital**'s growth and adapt to technological advancements.

1.5 Scope of the Problem:

This network infrastructure project is critical for **Al-Shifa Hospital** to achieve secure and compliant operations within the healthcare industry. The project's design prioritizes reliable connectivity, data protection, and future scalability, which together enable the hospital to navigate the challenges of a regulated environment with confidence. With a strong focus on security, the infrastructure supports seamless healthcare operations, fosters patient trust, and establishes a foundation for sustainable growth.

1.6 Significance of the Problem:

A well-designed network, even in simulation, plays a vital role in demonstrating the critical nature of healthcare operations. This project will simulate how an advanced network can improve patient care, streamline administrative tasks, and ensure

compliance with healthcare regulations. The use of Packet Tracer allows for the design and testing of a scalable and secure network that can serve as a model for real-world deployment.

1.7 Conclusion:

In summary, the **Al-Shifa Hospital Network Infrastructure** project is an essential undertaking for **Al-Shifa Hospital**. By addressing critical needs in security, connectivity, and scalability, this project aligns with the hospital's mission to provide reliable, efficient, and compliant healthcare services. The groundwork laid in this introduction sets the stage for the detailed design, implementation, and security protocols that will follow in this documentation.

Chapter II: Project Requirements and Analysis

2.1 Functional Requirements

The **Al-Shifa Hospital Network Infrastructure** project aims to provide a secure, scalable, and efficient network environment for **Al-Shifa Hospital**'s main hospital building. The key functional requirements are as follows:

- **Data Security:** Implement robust security protocols to protect sensitive healthcare data from internal and external threats. This includes encryption for data in transit, access control lists (ACLs), and secure authentication methods.
- **Inter-department Connectivity:** Establish seamless, high-performance connectivity between hospital departments to support efficient, real-time communication across all operations. This involves implementing site-to-site VPNs and redundancy measures to prevent connectivity disruptions.
- **Regulatory Compliance:** Ensure the network meets the regulatory requirements of the healthcare industry, including data protection standards

and secure data handling practices, to foster compliance and maintain the hospital's reputation.

These functional requirements form the backbone of the network's design, ensuring that the infrastructure supports **Al-Shifa Hospital**'s operational goals, protects patient data, and adheres to healthcare regulations.

2.2 Technical Specifications

The technical specifications outline the core hardware, software, and configurations required to achieve the project's functional requirements. Below is a list of the key network devices, including their roles and descriptions.

Network Devices:

- **Core Routers (Cisco 2901):**
  - **Quantity:** 2
  - **Role:** These routers serve as the primary inter-department connectivity solution, handling core routing tasks to enable secure communication between departments. Configured with OSPF and EIGRP for dynamic routing, they provide both scalability and efficient route convergence.

VOIP Router (Cisco 2811):

- **Quantity:** 1
- **Role:** This router is dedicated to managing the VOIP traffic for **Al-Shifa Hospital**. It connects the VOIP devices within the hospital to the network, ensuring high-quality voice communication across the system. It is configured with VOIP-specific protocols and supports voice gateways, enabling secure and efficient voice calls

between departments and remote locations. Additionally, it integrates with the core network routers for seamless communication between voice and data systems.

-

- **Core Switches (Cisco Catalyst 3650)**:
- **Quantity**: 2
- **Role**: The core switches are responsible for VLAN distribution and highspeed data transfer within each location. Positioned at the core of the network, these switches handle large volumes of traffic and support VLAN trunking to ensure seamless communication across departments.

- **Access Switches (Cisco Catalyst 2960)**:
- **Quantity**: 17

- **Role**: The access switches connect end-user devices to the network, enabling VLAN segmentation and providing fast data transfer. Configured with access control lists and port security, these switches ensure secure access at the edge of the network.

- **Wireless LAN Controller (WLC)**:
- **Role**: The WLC manages lightweight access points to provide wireless connectivity throughout the HQ and branch locations. It offers centralized control over SSIDs, channel assignment, and security policies, ensuring seamless and secure wireless access across the network.

- **Lightweight Access Points:**
- **Role:** Deployed across the HQ and branch locations, these access points provide wireless coverage, extending network access to mobile users. They are centrally managed by the WLC, ensuring consistent configurations and security.

- **Servers:**
  - **DHCP Server**: Responsible for dynamically assigning IP addresses to network devices, this server ensures efficient IP management across HQ and branch locations. It supports network scalability by managing IP pools for multiple VLANs.

- **DNS Server**: The DNS server translates domain names to IP addresses, facilitating access to internal and external resources. It is essential for efficient network navigation and service discovery.
- **NTP Server**: The NTP server synchronizes the clocks of all network devices, ensuring time consistency across HQ and branch locations. Accurate timekeeping is critical for logging, security audits, and troubleshooting. ○ **Syslog Server:** Centralized logging server that collects and stores log data from routers, switches, and other network devices. It provides critical data for network monitoring, security auditing, and issue diagnosis.
- **Web Server:** Hosts internal websites and web applications used by bank employees, enabling access to shared resources, documentations, and company portals.
- **Email Server:** Manages and stores emails for bank employees, ensuring secure and reliable internal and external communication. Configured to support security policies like encryption and spam filtering.

- **Configurations:**
  - **VLAN Segmentation:** Each department's traffic is segmented into its own VLAN, enhancing security and simplifying network management.
  - **Routing Protocols**: OSPF is configured for dynamic, scalable routing within HQ and branch, while EIGRP provides rapid route convergence.

- **Standards**: Adhere to IEEE 802.1Q standards for VLAN tagging and use IPsec for VPN security, with expanded configurations detailed in later sections.
- **Device Specifications Table:**

DEVICE TYPE	MODEL	QUANTITY	PRIMARY ROLE	DESCRIPTION
CORE ROUTER	Cisco 2901	2	Core routing, inter-branch connection	Manages routing between HQ and branches
CORE SWITCH	Cisco Catalyst 3650	2	Core switching, VLAN distribution	Handles highspeed core traffic and VLANs
ACCESS SWITCH	Cisco Catalyst 2960	17	Access layer for end-user connections	Provides connectivity and VLAN segmentation

WIRELESS LAN CONTROLLER	(Model based on WLC)	1	Manages wireless access points	Centralized control of WiFi network
LIGHTWEIGHT ACCESS POINTS	(Model based on AP)	Multiple	Extends wireless coverage	Provides wireless access to mobile devices
DHCP SERVER	N/A	1	IP address management	Assigns IPs dynamically
DNS SERVER	N/A	1	Domain name resolution	Maps domain names to IP addresses
NTP SERVER	N/A	1	Time synchronization	Ensures consistent timestamps
SYSLOG SERVER	N/A	1	Centralized logging	Collects logs for monitoring and audits
WEB SERVER	N/A	1	Hosts internal websites	Provides access to bank resources
EMAIL SERVER	N/A	1	Email management	Manages internal and external communication

2.3 **Assumptions and Constraints:**

The design and implementation of the **Al-Shifa Hospital** network are based on specific assumptions and constrained by a few critical factors:

Assumptions:

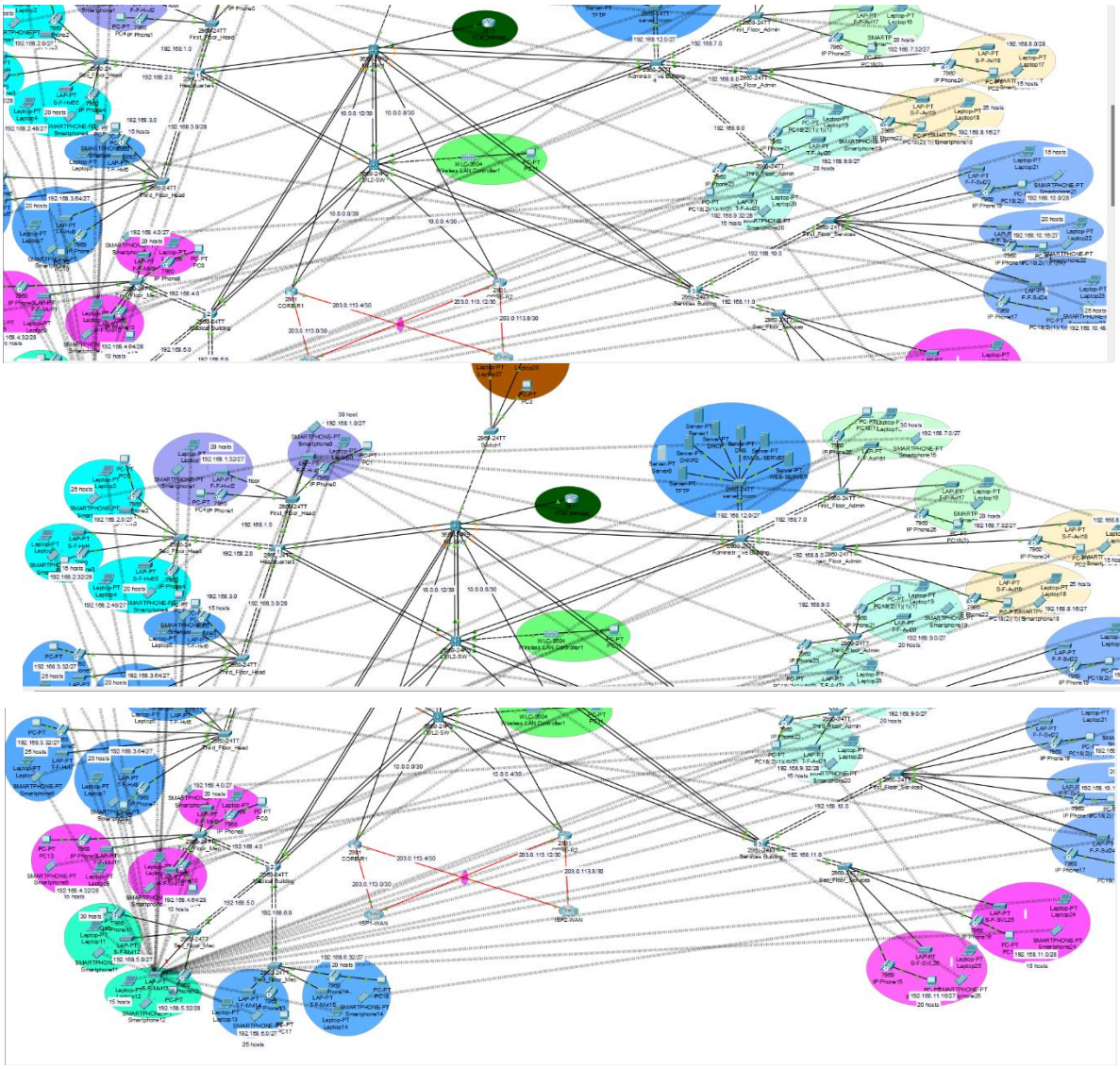
- The network will support the current estimated number of users and devices across the main hospital branch.
- All hospital personnel accessing the network will use devices compatible with Cisco network configurations.

Constraints:

- **Budget Limitations:** The project must remain within the allocated budget, which may affect the choice of certain hardware or advanced configurations.
- **Physical Installation Constraints:** The layout and available space at the hospital branch dictate certain design choices, especially concerning hardware placement and cabling.
- **Performance Constraints:** The network must meet minimum bandwidth and latency requirements to support hospital operations, medical applications, and real-time data access.

These assumptions and constraints provide the boundaries within which the network must be designed, ensuring optimal performance while aligning with **Al-Shifa Hospital's** budget and physical environment.

.Chapter III: Network Design and Architecture



3.3 Network Components:

This section provides detailed descriptions of the network components used in the FutureNet infrastructure. Devices are organized by type and location (HQ or branch) to clarify roles and placements.

Network Components Table:

Device Type			Model	Location
Core Router	Cisco 2901	HQ	External routing and interbranch connection	Manages external routing between the hospital and the internet, and routing between the hospital and branches
VoIP Router	Cisco 2811	HQ	VoIP handling	Handles VoIP traffic within the hospital, routing voice communications
Core Switch	Cisco Catalyst 3650	HQ	Core switching, VLAN distribution	Handles high-speed core traffic and VLAN segmentation
Access Switch	Cisco Catalyst 2960	HQ	Access layer for end-user connections	Provides connectivity and VLAN segmentation for the hospital network
Wireless LAN Controller	Cisco WLC Model	HQ	Manages wireless access points	Centralized control of the WiFi network across the hospital
Lightweight Access Points	Cisco AP Model	HQ	Extends wireless coverage	Provides wireless access to mobile devices and staff in the hospital
DHCP Server	N/A	HQ	IP address management	Dynamically assigns IP addresses to hospital devices

DNS Server	N/A	HQ	Domain name resolution	Maps domain names to IP addresses for hospital systems
NTP Server	N/A	HQ	Time synchronization	Ensures consistent timestamps across hospital systems
Syslog Server	N/A	HQ	Centralized logging	Collects logs for monitoring and audits of hospital network activity
Web Server	N/A	HQ	Hosts internal websites	Provides access to hospital resources, like patient data and internal forms

Each device is essential to supporting Al-Shifa Hospital's operational goals, providing the necessary connectivity, data management, and network services.

3.4 Naming and IP Addressing Scheme: A standardized naming and IP addressing scheme is used to simplify device identification and management, enhancing troubleshooting efficiency. Each department within Al-Shifa Hospital is assigned a unique VLAN, and devices within each VLAN are allocated IP addresses from specific subnet ranges.**IP Addressing Scheme Table:**
The IP addressing scheme assigns specific ranges to each VLAN, ensuring organized traffic segmentation and enhanced security. Device naming follows a structured convention, such as "HQ-SW-Core1" for HQ core switches and "BR-RT-Branch1" for branch routers.

Location	VLAN	Subnet	Usable IP Range	Default Gateway	Broadcast IP
Main HQ (1st Floor)	VLAN 10 (ER)	192.168.1.0/27	192.168.1.1 - 192.168.1.30	192.168.1.1	192.168.1.31
	VLAN 20 (Reception)	192.168.1.32/27	192.168.1.33 - 192.168.1.62	192.168.1.33	192.168.1.63
Main HQ (2nd Floor)	VLAN 30 (Admin)	192.168.2.0/27	192.168.2.1 - 192.168.2.30	192.168.2.1	192.168.2.31
	VLAN 40 (Doctors)	192.168.2.32/28	192.168.2.33 - 192.168.2.46	192.168.2.33	192.168.2.47
	VLAN 50 (Training)	192.168.2.64/27	192.168.2.65 - 192.168.2.94	192.168.2.65	192.168.2.95
Main HQ (3rd Floor)	VLAN 60 (Sections)	192.168.3.0/28	192.168.3.1 - 192.168.3.14	192.168.3.1	192.168.3.15

	VLAN 70 (Medical Ed.)	192.168.3.16/27	192.168.3.17 - 192.168.3.46	192.168.3.33	192.168.3.47
	VLAN 80 (Staff Rec.)	192.168.3.64/27	192.168.3.65 - 192.168.3.94	192.168.3.65	192.168.3.95
Medical Building (1st Floor)	VLAN 90 (OR)	192.168.4.0/27	192.168.4.1 - 192.168.4.30	192.168.4.1	192.168.4.31
	VLAN 100 (ICU)	192.168.4.32/28	192.168.4.33 - 192.168.4.46	192.168.4.33	192.168.4.47
	VLAN 110 (Labs)	192.168.4.64/28	192.168.4.65 - 192.168.4.78	192.168.4.65	192.168.4.79
Medical Building (2nd Floor)	VLAN 120 (Wards)	192.168.5.0/27	192.168.5.1 - 192.168.5.30	192.168.5.1	192.168.5.31
	VLAN 150 (Special Units)	192.168.6.32/27	192.168.6.33 - 192.168.6.62	192.168.6.33	192.168.6.63
Medical Building (3rd Floor)	VLAN 160 (Core Admin)	192.168.7.0/27	192.168.7.1 - 192.168.7.30	192.168.7.1	192.168.7.31
	VLAN 170 (Reception)	192.168.7.32/27	192.168.7.33 - 192.168.7.62	192.168.7.33	192.168.7.63
Admin Building (1st Floor)	VLAN 180 (HR)	192.168.8.0/28	192.168.8.1 - 192.168.8.14	192.168.8.1	192.168.8.15
	VLAN 190 (Archives)	192.168.8.16/27	192.168.8.17 - 192.168.8.46	192.168.8.33	192.168.8.47

Admin Building (2nd Floor)	VLAN 200 (Employee Mgmt.)	192.168.9.32/28	192.168.9.33 - 192.168.9.46	192.168.9.33	192.168.9.47
	VLAN 210 (Storage)	192.168.9.32/28	192.168.9.33 - 192.168.9.46	192.168.9.33	192.168.9.47
Services Building (1st Floor)	VLAN 220 (Food)	192.168.10.0/28	192.168.10.1 - 192.168.10.14	192.168.10.1	192.168.10.15
	VLAN 230 (Maint.)	192.168.10.32/27	192.168.10.33 - 192.168.10.62	192.168.10.33	192.168.10.63
	VLAN 240 (Additional Food)	192.168.10.64/27	192.168.10.65 - 192.168.10.94	192.168.10.65	192.168.10.95
Server Room	VLAN 250 (Servers)	192.168.12.0/27	192.168.12.1 - 192.168.12.30	192.168.12.1	192.168.12.31

3.5 Redundancy and High Availability:

To ensure high availability and minimal downtime, the network incorporates redundancy mechanisms using both HSRP (Hot Standby Router Protocol) and EtherChannel. HSRP provides router redundancy, allowing a backup router to take over in case the primary router fails. EtherChannel, configured on core switches, offers link redundancy by bundling multiple Ethernet links, which increases bandwidth and provides a failover path.

These redundancy measures ensure that Al-Shifa Hospital's network remains resilient and able to maintain uninterrupted service, even in the event of a device or link failure. The hospital’s network infrastructure has been designed to prevent single points of failure and ensure continuous connectivity for critical healthcare applications.

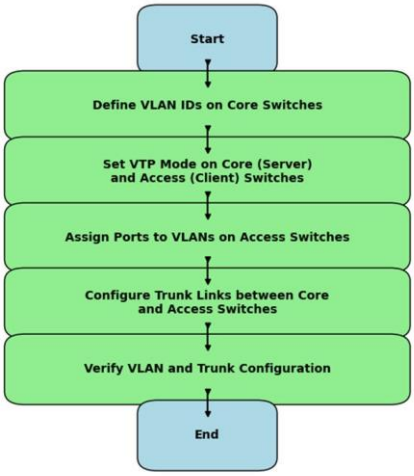
Chapter IV: Network Configuration and Implementation

4.1 Layer 2 Configuration:

The Layer 2 configuration for Al-Shifa Hospital's network establishes VLANs to ensure proper traffic segmentation and basic loop prevention to maintain a stable network environment.

- **VLAN Configuration**: VLANs are configured centrally on the core switches, with VTP (VLAN Trunking Protocol) used to propagate VLAN information to access switches. This centralized approach simplifies VLAN management and ensures consistent VLAN availability across the network.
- **Spanning Tree Protocol (STP)**: Standard STP is configured to prevent network loops. STP ensures that only the necessary paths are active at any given time, maintaining network stability and reducing potential broadcast storms.

Since **Al-Shifa Hospital** is a single branch facility, the network design is focused on supporting the operations within this single location, ensuring high availability, and redundancy while maintaining efficient traffic segmentation and loop-free paths.



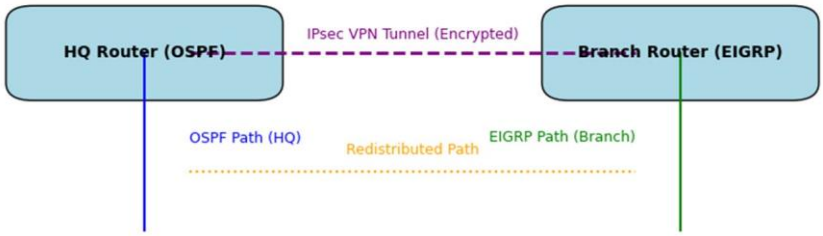
A flowchart showing steps to configure VLANs, assign ports, and configure trunks.

4.2 Layer 3 Configuration:

Layer 3 configuration in Al-Shifa Hospital's network ensures efficient routing within the main hospital location, providing dynamic routing between subnets and secure communication.

- **Routing Protocols:**
  - **OSPF** is implemented internally within the hospital's core network to dynamically manage routing between subnets.

These routing protocols ensure efficient data transmission across the hospital’s network, allowing seamless communication between the various VLANs and ensuring fast and reliable connectivity for critical healthcare applications.



A diagram illustrating main routing paths and VPN setup steps for inter-branch communication.

4.3 Access Control Lists (ACLs):

General network-wide ACLs are configured to control traffic flow, ensuring only authorized data passes between network segments. The table below summarizes key ACLs and their actions.

ACL Name	Action	Source	Destination	Description
ACL_Allow_Internal	Permit	Internal VLANs	Internal VLANs	Allows traffic between internal VLANs
ACL_Deny_External	Deny	External Networks	Sensitive VLANs	Blocks external access to sensitive data
ACL_Admin_Only	Permit	Admin VLAN	Management VLAN	Restricts management access to admins only

These ACLs ensure secure traffic flow and prevent unauthorized access to critical areas within the network.

4. Device security in Al-Shifa Hospital's network is essential to ensure that unauthorized access to critical network equipment is prevented. The following security measures are implemented:

- **Password Protection:** Strong passwords are configured on administrative accounts of network devices to ensure that only authorized personnel can access and manage the equipment.
- **Port Security:** Port security settings are applied on access switches to limit the number of MAC addresses per port. This prevents unauthorized devices from connecting to the network.
- **SSH Configuration:** SSH (Secure Shell) is enabled on all network devices for secure remote management. This ensures that data transmitted during remote sessions is encrypted and protected from potential interception.

- **Role-based Access Control (RBAC):** RBAC is implemented to define specific access levels for users, ensuring that only authorized personnel can access sensitive network management functions.

Device Type	Location	Port Security	SSH Setup	Additional Security Settings
Core Router	HQ	N/A	SSH enabled, port 22	Strong password policy, ACLs for management access
Core Router	Branch	N/A	SSH enabled, port 22	Strong password policy, ACLs for management access
Core Switch	HQ	Enabled on user-facing ports	SSH enabled, port 22	Port security to restrict MAC addresses; ACLs for management VLAN
Access Switch	HQ, Branch	Enabled on all userfacing ports	SSH enabled, port 22	MAC address limit set per port, shutdown on violation
Wireless LAN Controller (WLC)	HQ	N/A	SSH enabled, port 22	Role-based access control, WPA2 for wireless encryption
DHCP Server	HQ	N/A	Disabled (local access only)	Restricted to internal VLAN only
DNS Server	HQ	N/A	Disabled (local access only)	DNSSEC for secure queries, restricted to internal network
Web Server	HQ	N/A	Enabled for remote management	SSL/TLS for secure web access

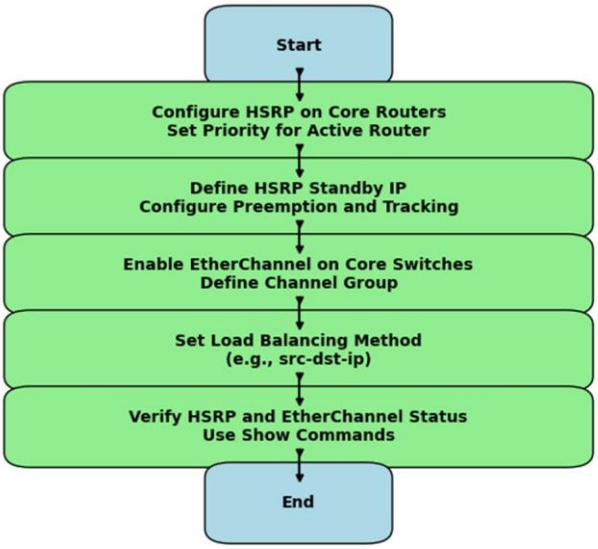
Email Server	HQ	N/A	Enabled for remote management	SSL/TLS for email encryption
Syslog Server	HQ	N/A	Disabled (local access only)	Internal logging restricted to management VLAN

A table summarizing security configurations for each key device, including port security and SSH setup.

4. To ensure continuous operation and minimize downtime, Al-Shifa Hospital's network incorporates redundancy mechanisms using HSRP and EtherChannel.

- **HSRP Configuration:** HSRP is configured to provide router redundancy. One router is set as the active router, while the other is the standby router. If the active router fails, the standby router automatically takes over, ensuring uninterrupted connectivity.
- **EtherChannel:** EtherChannel is implemented on the core switches to combine multiple Ethernet links into a single logical link. This increases the available bandwidth and provides link redundancy. If one link fails, traffic is automatically rerouted through the remaining active links, ensuring continuous service.

.



A flowchart showing HSRP and EtherChannel configuration steps to enable failover and link redundancy