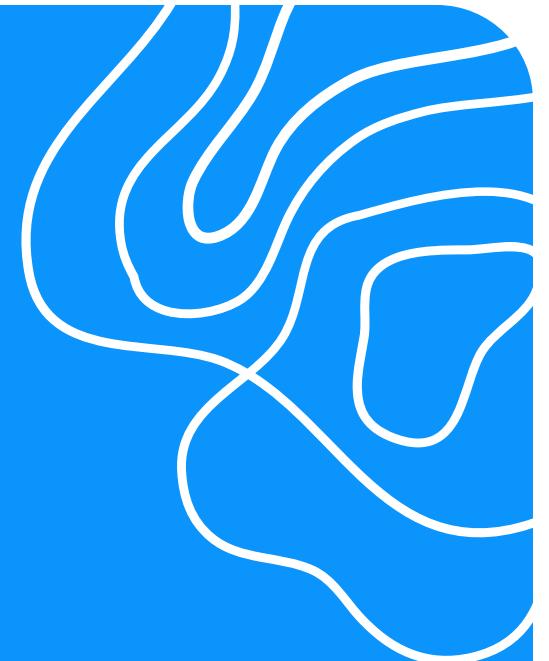


# HOSPITAL SYSTEM NETWORK DESIGN

---

*proposal*



# ABOUT US

1

Mohamed Essam Mohamed  
Elabd

2

Yahya Mahmoud Mousa El  
said

3

Karim Rushdy Mousa  
abdelhameed

4

Shawky El Sayed Ibrahim  
Ibrahim Elmahdy

5

Mohamed mahros Elsayed  
radwean



# TEAM MEMBERS & TASKS



**Mohamed Essam Mohamed Elabd:** Project Lead, VLAN Configuration, and Security Implementation.



**Yahya Mahmoud Mousa El Said:** IP Addressing and OSPF Routing.



**Karim Roshdy Mousa Abdelhameed:** Subnetting and Site-to-Site VPN.



**Shawky Elsayed Ibrahim Ibrahim Elmahdy:** Inter-VLAN Routing and ACLs.



**Mohamed Mahros Elsayed Radwean:** Port Security and System Monitoring.

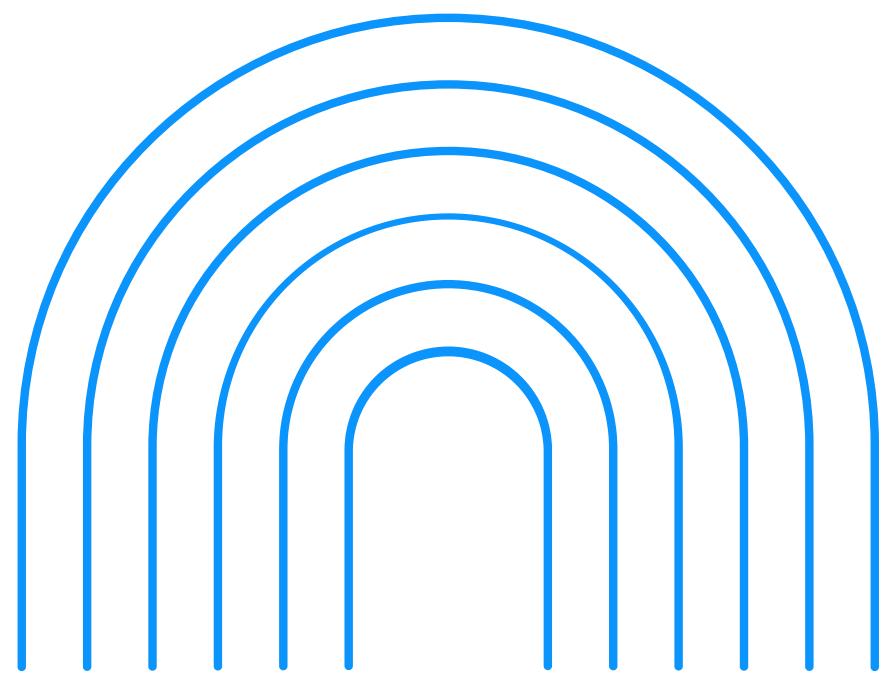
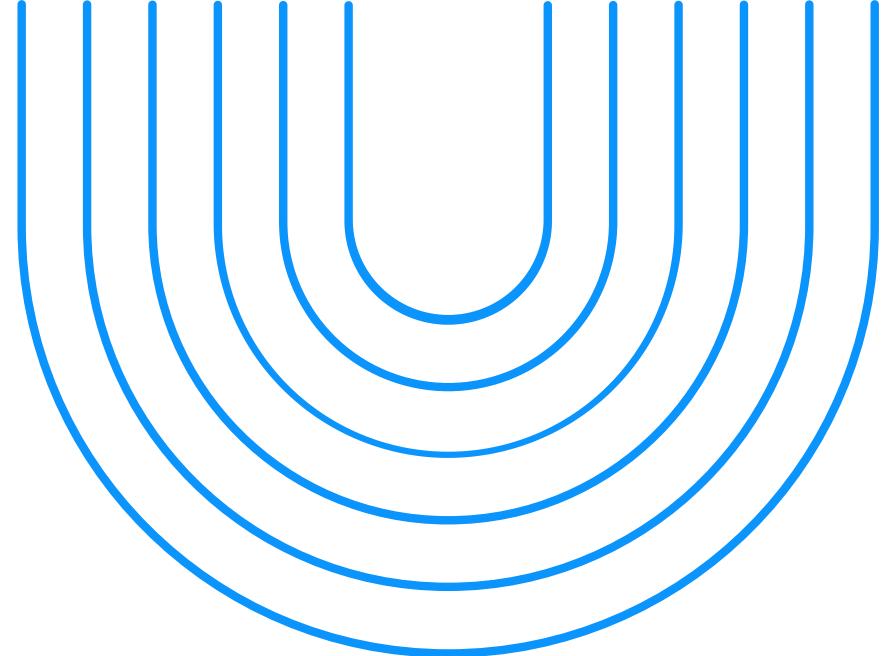


**Course Track: Cisco Cybersecurity Engineer**  
**Advisor: Eng. Mamdouh Al-Tahiry**

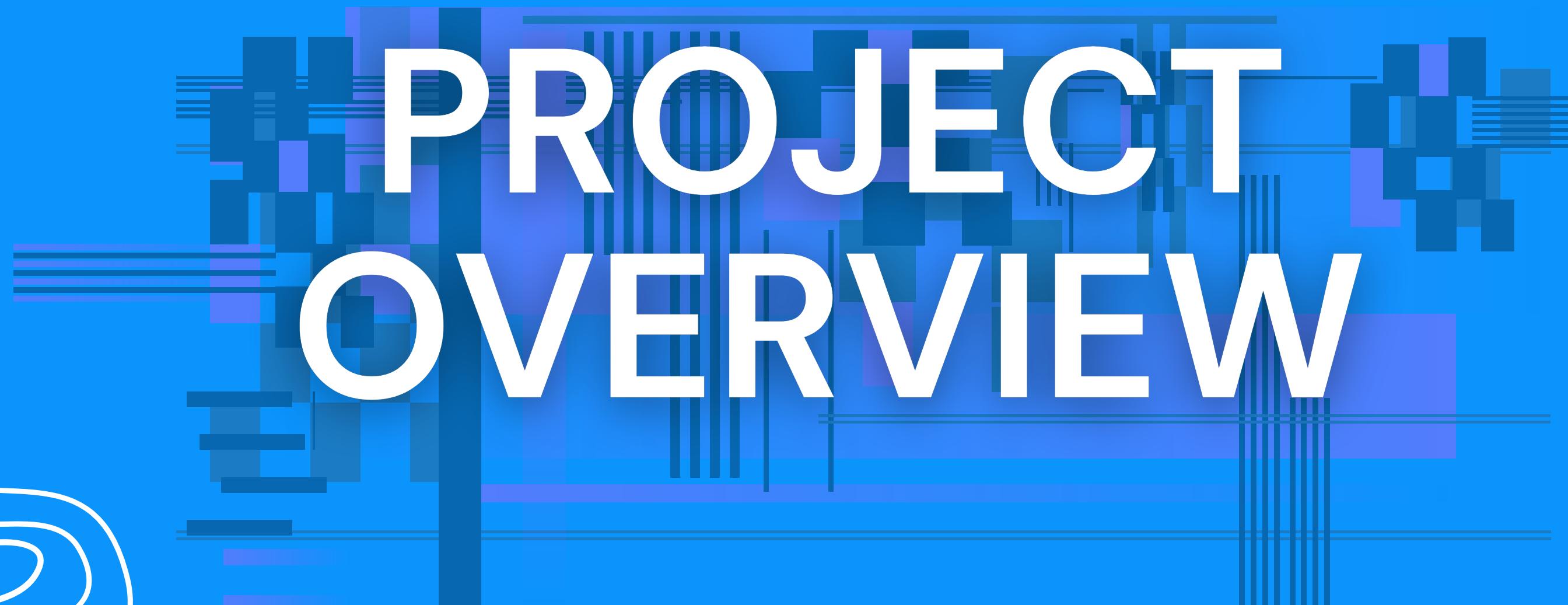
# TABLE OF CONTENT



- 01.** PROJECT OVERVIEW
- 02.** GOALS
- 03.** BUSINESS MODEL
- 04.** PROJECT PHASES & RESULTS



# PROJECT OVERVIEW



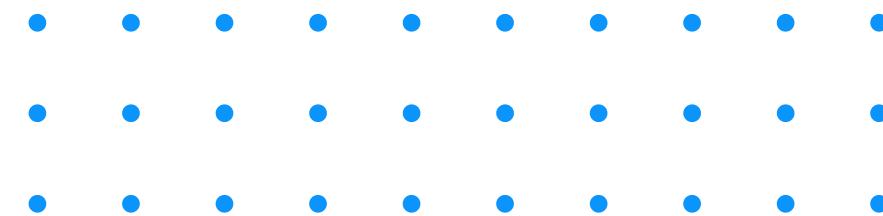
01. OBJECTIVE
02. DESCRIPTION
03. TOOLS USED



## 01. OBJECTIVE

---

To design and implement a secure, efficient, and scalable network infrastructure for Health Services, ensuring reliable communication, data management, and future scalability.





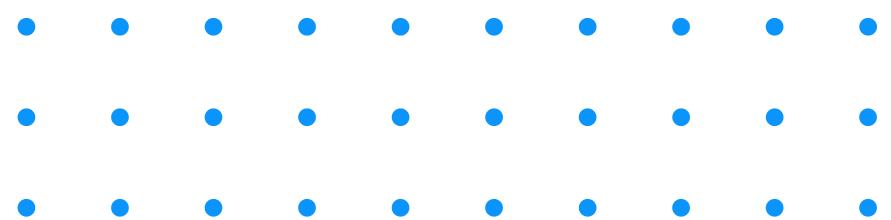
## 02. **DESCRIPTION**

---

This project involves the development of a modern, secure network across two locations (headquarters and branch) using VLANs, OSPF, IPsec VPN, ACLs, and other security protocols to ensure data integrity and efficiency.

# 03. TOOLS USED

- ✓ Cisco Packet Tracer: To simulate the network design and configurations.
- ✓ OSPF: For dynamic routing between departments and locations.
- ✓ VLAN: To separate network traffic and enhance security.
- ✓ ACLs, IPsec VPN, and Port-Security: To ensure secure and encrypted communication.





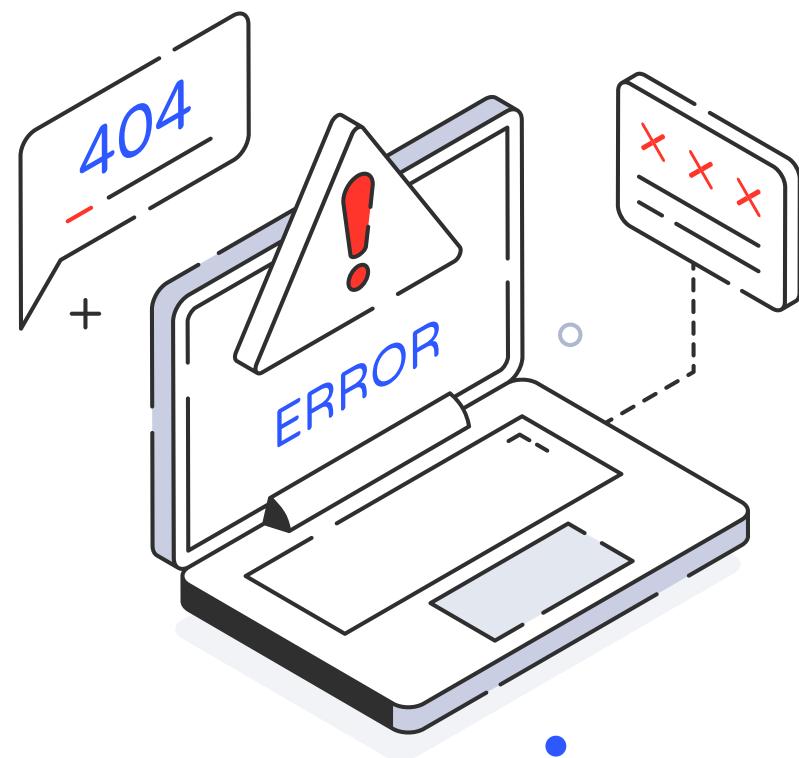
# GOALS

- O1. BEFORE THE PROJECT
- O2. AFTER THE PROJECT
- O3. SECURITY & EFFICIENCY IMPROVEMENTS

# 01. BEFORE THE PROJECT



The hospital's paper-based system was inefficient, leading to delays in communication and patient care.



**poor network with No VLANs or security protocols:** The existing network setup lacked segmentation, making it vulnerable to data breaches and inefficiencies.

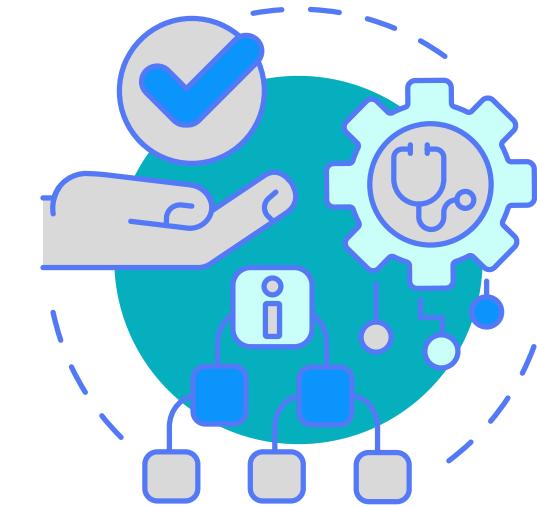


**Challenges:** Security risks, lack of scalability, and reliance on third-party IT services for data management.

## 02.GOALS – AFTER THE PROJECT



**Advanced Security:**  
Segmentation using  
VLANs, data  
encryption with IPsec  
VPN, and access  
control using ACLs and  
Port-Security.



**Scalability:** Easily  
scalable network  
infrastructure that  
can support future  
growth.



**Efficiency:** Faster  
communication  
between departments,  
reducing patient wait  
times and improving  
healthcare delivery.



**Centralized  
Management:**  
Streamlined network  
management using  
OSPF for dynamic  
routing and DHCP for  
IP addressing.

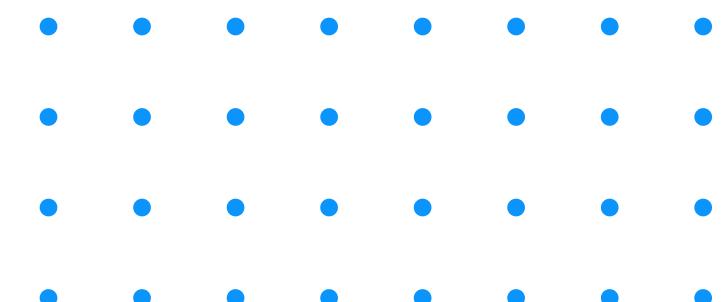
# 03.GOALS – ENHANCED SECURITY



VLAN segmentation to separate traffic and protect sensitive information.

IPsec VPN for encrypted communication between headquarters and branch.

ACLs to control access to sensitive resources and network segments.



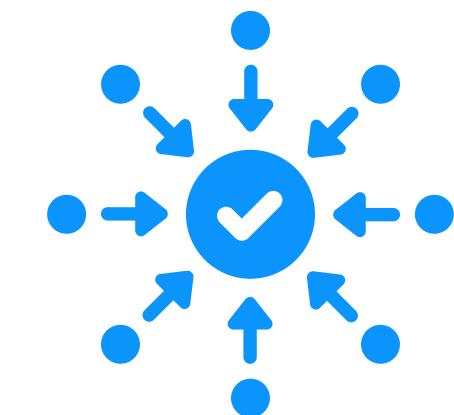
## 04. GOALS – IMPROVED NETWORK MANAGEMENT



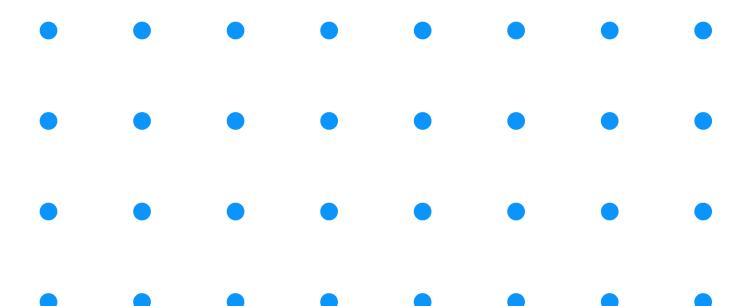
**Use of dynamic IP allocation through DHCP servers.**



**OSPF protocol for seamless and efficient routing across all departments and locations.**



**Centralized network control, simplifying troubleshooting and performance monitoring.**



## **05.GOALS – BETTER COMMUNICATION & EFFICIENCY**

**Better Communication:** Faster, more reliable communication between the headquarters and branch locations.

Departments can interact securely and efficiently across separate VLANs.

**Efficiency Gains:**  
Reduced operational downtime, leading to enhanced patient care and faster administrative processes.

# BUSINESS MODEL



01. MAIN PROBLEMS
02. KEY ACTIVITIES
03. VALUE PROPOSITION

## 03. BUSINESS MODEL MAIN PROBLEMS

**Reliance on a paper-based system, which slowed down operations.**

**Lack of secure communication across departments and locations.**

**Inefficient IT management using third-party services.**

**Data vulnerabilities due to the lack of security protocols.**

# 03. BUSINESS MODEL KEY ACTIVITIES

**Designing a secure network infrastructure tailored to healthcare needs.**

**Testing the network for reliability, security, and performance.**

**Configuring VLANs, OSPF, IPsec VPN, ACLs, and port-security protocols.**

**Maintaining and monitoring the network for future scalability and enhancements.**

# 03. BUSINESS MODEL REVENUE & COSTS

**Revenue:** The hospital saves on operational costs by internalizing IT management, reducing dependency on third-party services.

**Costs:** Initial investments include network hardware (routers, switches), software, and training for staff to manage the system.

# 03. BUSINESS MODEL KEY PARTNERS

**Cisco:** For network hardware and software support.

**Internet Service Providers (ISPs):** For redundant connections to ensure uptime and availability.

**Security Experts:** To consult on implementing the best practices for network security in a healthcare environment.

# **03. BUSINESS MODEL RESOURCES**

**Human Resources:** Network engineers and IT staff to maintain and manage the system.

**Hardware & Software:** Routers, switches, servers, and network simulation tools.

**Security Tools:** Encryption software, VPN tools, and monitoring tools.

# **03. BUSINESS MODEL VALUE PROPOSITION**

**The hospital network provides secure, scalable, and efficient communication across departments, improving patient care and operational performance.**

**Reduces costs by eliminating third-party IT service dependencies and allows for future scalability.**

# **03. BUSINESS MODEL TARGET CUSTOMERS**

**Primary Users:** Internal hospital staff, including administrative and medical personnel.

**Secondary Users:** IT staff responsible for managing the network.

**Patients:** Indirect beneficiaries due to faster and more secure healthcare services.

# OUR STRATEGY

## Goal

Establish a robust and secure hospital network infrastructure to enhance patient care and streamline operations.

### Marketing

Promote the hospital's technological advancements and patient care quality through targeted marketing strategies.

#### Online

Utilize social media and the hospital website to share success stories, patient testimonials, and innovative services.

#### Offline

Engage with the community through health fairs and local events to increase awareness about the hospital's services and technology.

### Partnership

Collaborate with technology providers and healthcare organizations to optimize network solutions and services.

#### Brands

Partner with leading medical technology brands to integrate advanced healthcare solutions into the hospital network.

#### Affiliates

Collaborate with local healthcare providers to enhance referral networks and improve service offerings.

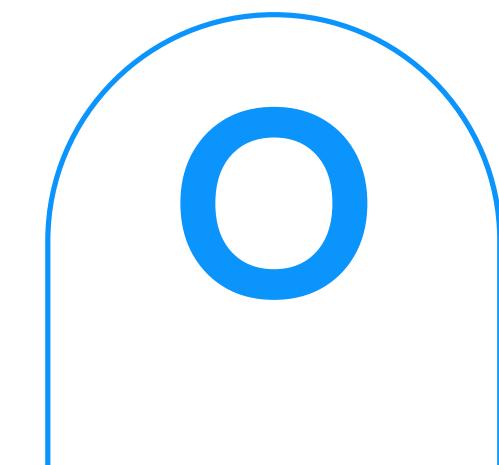
**S**

## STRENGTHS

- Advanced technology infrastructure enhancing patient care.
- Experienced IT team ensuring smooth network operations.
- Strong partnerships with medical technology providers.

- Expansion of telemedicine services to reach more patients.
- Potential to attract more healthcare partnerships.

## OPPORTUNITIES

**O****W**

## WEAKNESSES

- Initial high costs for network implementation and training.
- Dependence on technology, which may lead to operational risks during outages.

- Rapid technological changes requiring continuous updates.
- Increased competition from other healthcare providers adopting similar technologies.

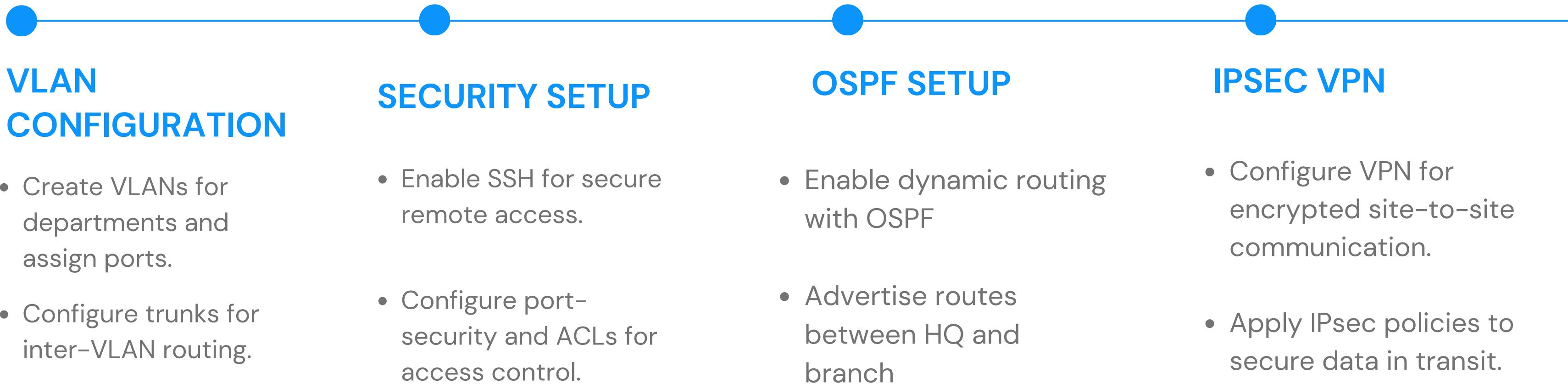
## THREATS

**T**

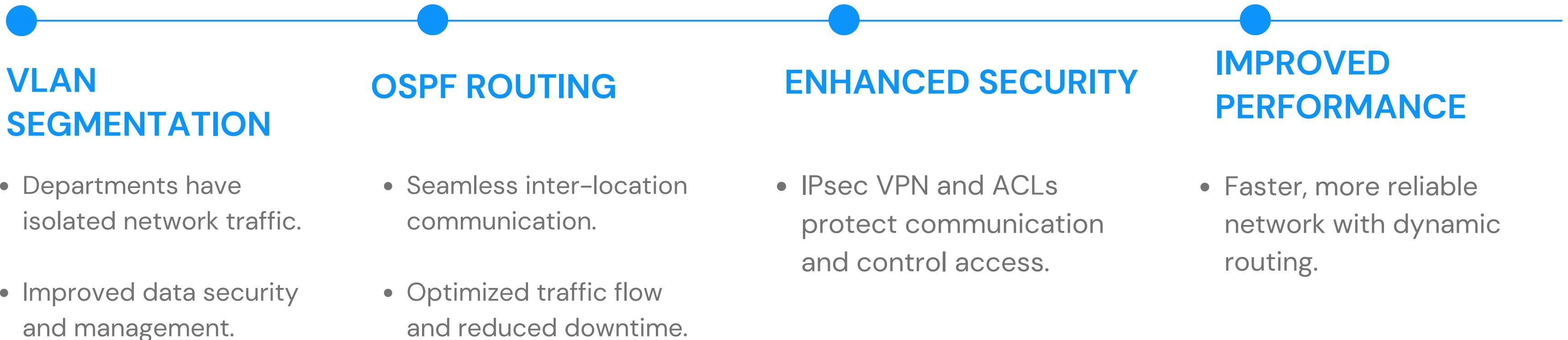
# PROJECT PHASES & RESULTS

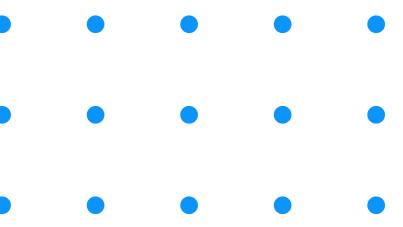
- 01. PHASES OF CONFIGURATION
- 02. NETWORK INFRASTRUCTURE
- 03. RESULTS & OUTPUT

# PHASES OF CONFIGURATION



# PHASES OF CONFIGURATION





# CONCLUSION

---

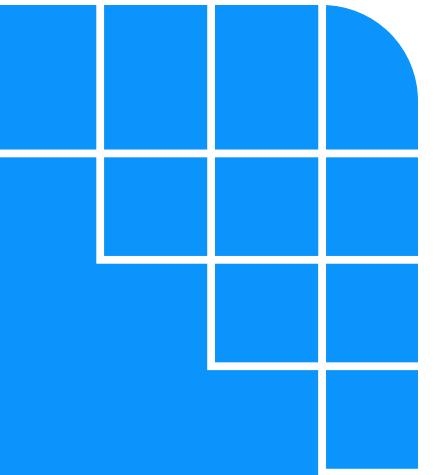
The project successfully designed and implemented a secure, scalable, and efficient network infrastructure for Melbourne Health Services.

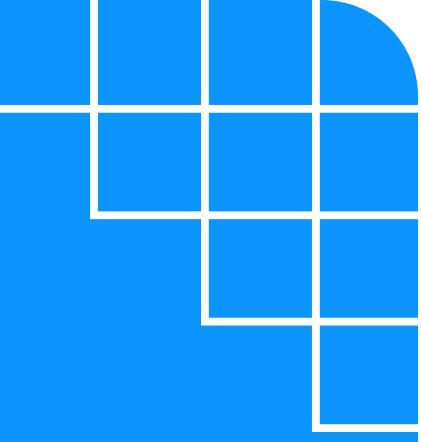
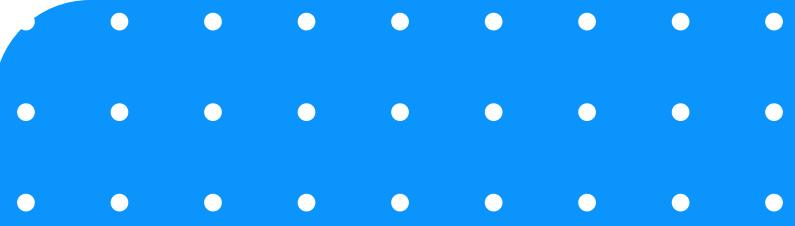
The hospital now has a system that ensures fast communication, high data security, and the ability to scale as needed.

# PACKET TRACER

[GO TO PROJECT](#)

01. PHASES OF CONFIGURATION
02. NETWORK INFRASTRUCTURE
03. RESULTS & OUTPUT





Do you have any question?

---

# THANK YOU

---

