CN PROJECT TITLE

08/12/2024

Secure Healthcare Project

MUHAMMAD SOHAIB RAFIQ
MUHAMMAD AYAN
FAHAD FAISAL

PHASE 2

OBJECTIVE

- To design and implement a secure, scalable, and robust network infrastructure ensuring high performance, redundancy, and availability.
- The network will safeguard data confidentiality, integrity, and availability while supporting the healthcare's growing user base and operational needs.

SCOPE

The project encompasses the design and deployment of the entire network infrastructure for Healthcare , addressing the following key areas:

1 LAN and WLAN

2 Voice Network

3 Firewall and Security

4 Data Center

5 Cloud Integration

6 High Availability

7 Routing and Switching

8 Testing and Validation

DELIVERABLES

1	Fully Configured Network Infrastructure Based on the Hierarchical Design Model
2	Configured VLANs, IP Addressing, Inter-VLAN Routing, DHCP, and OSPF
3	Functional VoIP System and Telephony Services
4	Configured Cisco ASA Firewall with Defined Security Policies
5	Documentation of Network Design, Configurations, and Testing Results
6	Network Topology Diagram and Configuration Files for Reference
7	A Final Report Detailing the Implementation Process, Challenges Faced, and Solutions Provided

Our Group

MUHAMMAD AYAN

PHASE 1 IMPLEMENTATION +
Contribution to other Phases

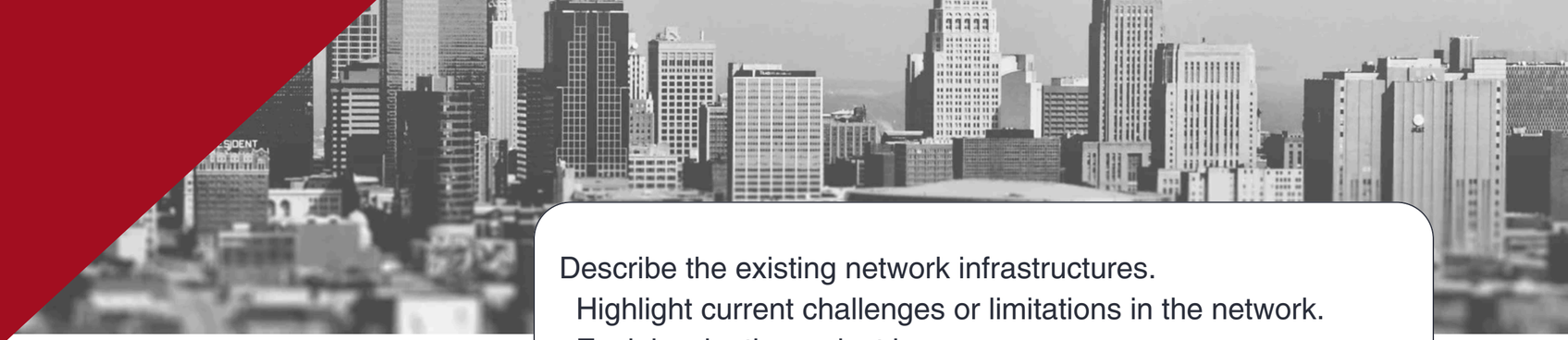
FAHAD FAISAL

PHASE 2 IMPLEMENTATION
+Contribution to other Phases

MUHAMMAD SOHAIB RAFIQ

PHASE 3 IMPLEMENTATION+
Contribution to other Phases

2 Background and Problem Statement



Describe the existing network infrastructures.
Highlight current challenges or limitations in the network.
Explain why the project is necessary.

Current Challenges and Limitations:

Why Secure Healthcare, Clinics, and Hospitals Are Necessary

Phase 2

3. Proposed Solution

Outline the proposed network design.

The proposed secure healthcare network is designed with a focus on redundancy, scalability, and security, integrating advanced Cisco technologies and protocols to create a robust infrastructure capable of handling healthcare data and applications.

Outline the proposed network design.

Cisco Technologies Used

- **Cisco ISR 4331 Routers (x2)**
- **Cisco 2811 Router**
- **Cisco 2960-24 Switches (x9)**
- **Cisco 3560-24PS Multi-Layer Switches (x2)**
- **Cisco Firewall ASA 5506**
- **Cisco WLC 2504**
- **Cisco LAP-PT (x7)**
- **HSRP (Hot Standby Router Protocol)**
- **EtherChannel**

VoIP (Cisco 2811 Router)

Ephone Protocol

Phase 2

3. Proposed Solution

Outline the proposed network design.

The proposed secure healthcare network is designed with a focus on redundancy, scalability, and security, integrating advanced Cisco technologies and protocols to create a robust infrastructure capable of handling healthcare data and applications.

Network Protocols and Tools

- **OSPF (Open Shortest Path First)**
- **VLANs (Virtual Local Area Networks)**
- **ACLs (Access Control Lists)**
- **Password Encryption**
- **No IP Domain Lookup**

Tools:

- Cisco Packet Tracer

Budget Estimation

- Lower Range:

PKR 7,840,000

- Upper Range:

PKR 14,560,000

Budget Estimation for Network Devices

NOTE: This Estimation is without end devices

7. Testing & Evaluation

Test Type	Objective	Test Method
Connectivity Test	Verify network devices are properly connected	Ping Test, Traceroute
Redundancy Testing	Ensure failover and backup mechanisms work	Test HSRP and EtherChannel Failover
ACL Testing	Verify that ACLs restrict or allow access as intended	Attempt unauthorized access and confirm blocking
Firewall Testing	Ensure firewall is filtering traffic correctly	Test inbound/outbound traffic through ASA 5506
VoIP Connectivity	Ensure VoIP works over the network	Test call quality and routing via Cisco 2811

8. Risk Assessment

Risk Type	Description	Mitigation Strategy	Impact Level (High/Medium/Low)
Hardware Failure	Failure of critical hardware like routers, switches, or firewalls.	Keep spare equipment, implement regular hardware maintenance, and set up redundant systems.	**High**
Configuration Errors	Incorrect device configurations leading to network downtime or security breaches.	Implement change management, configuration backups, and regular configuration audits.	**High**

8. Risk Assessment

Risk Type	Description	Mitigation Strategy	Impact Level (High/Medium/Low)
Security Breach (Cyber Attack)	Network vulnerabilities exploited by attackers (e.g., DoS, ransomware, phishing).	Deploy advanced firewalls (Cisco ASA 5506), ACLs, encryption, and IDS/IPS systems for real-time threat detection.	**High**
Network Congestion	Excessive traffic causing network slowdowns, particularly during peak	Optimize network design with proper VLAN segmentation.	Medium

8. Risk Assessment

Risk Type	Description	Mitigation Strategy	Impact Level (High/Medium/Low)
Disaster Recovery Failures	Failure of backup systems or disaster recovery protocols in case of system failure.	Test backup and recovery systems regularly, implement off-site backups, and maintain an up-to-date disaster recovery plan.	**High**
IoT Device Vulnerabilities	Security issues in IoT devices, which are often less secure than other network devices.	Isolate IoT devices in separate VLANs, regularly update device firmware	Medium

CONCLUSION

In summary, the proposed network design not only meets the current needs of the healthcare facility but also positions it for future growth, scalability, and compliance with regulatory standards.

With robust security, high availability, and performance optimization, this solution will provide healthcare providers with the necessary tools to protect sensitive patient data, maintain network uptime, and improve overall operational efficiency.

The network is resilient to both internal and external threats, ensuring that healthcare services can continue without disruption, even in the face of cyberattacks or system failures.