A Case Study Report on

"Server Infrastructure Analysis at KLES Dr. Prabhakar Kore Hospital & Medical Research Centre, Belagavi"

A Case Study Report Submitted for the Course of
Computer Networks-2 (23ECSC303) in
6th Semester of Computer Science and Engineering

by

Chinmay Prabhu 02FE22BCS026

Harsh Nesari 02FE22BCS040

Hritik Satnaik 02FE22BCS041

Mahmad Suhan Jamadar 02FE22BCS048

Qadir Terniker 02FE22BCS053

Under the guidance of

Dr. Satish Bhojannawar
Professor,
Department of Computer Science and Engineering, KLE Technological University's Dr. MSSCET, Belagavi.

KLE Technological University's
Dr. M. S. Sheshgiri College of Engineering and Technology,Belagavi – 590 008.

April 2025

College of Engineering & Technology, Udyambag, Belagavi - 590 008, Karnataka, India
Ph.: 0831 - 2443881,82,83,0831-2440322 | Fax:0831-2441644| principal@klescet.ac.in | www.klescet.ac.in

DECLARATION

We hereby declare that the matter embodied in this report entitled "**Server Infrastructure Analysis at KLES Dr. Prabhakar Kore Hospital & Medical Research Centre, Belagavi**" submitted to KLE Technological University for the course completion of Computer Networks-2 ((23ECSE303) in the 6th Semester of Computer Science and Engineering is the result of the work done by us in the Department of Computer Science and Engineering, KLE Dr.M. S. Sheshgiri College of Engineering, Belagavi .We further declare that to the best of our knowledge and belief, the work reported here in doesn't form part of any other project on the basis of which a course or award was conferred on an earlier occasion on this by any other student(s), also the results of the work are not submitted for the award of any course, degree or diploma within this or in any other University or Institute. We hereby also confirm that all of the experimental work in this report has been done by us.

Belagavi – 590 008
Date :

Chinmay Prabhu
(02FE22BCS026)

Harsh Nesari
(02FE22BCS040)

Hritik Satnaik
(02FE22BCS112)

Suhan Jamadar
(02FE22BCS048)

Qadir Terniker
(02FE22BCS053)

College of Engineering & Technology, Udyambag, Belagavi - 590 008, Karnataka, India
Ph.: 0831 - 2443881,82,83,0831-2440322 | Fax:0831-2441644| principal@klescet.ac.in | www.klescet.ac.in

Table of Contents

1.Introduction

This case study explores the computer network setup at KLES Dr. Prabhakar Kore Hospital and Medical Research Centre, Belagavi, and explains how it plays a key role in supporting the hospital's daily activities. In a healthcare environment where timely access to information can directly impact patient care, having a reliable and secure network is extremely important. The hospital relies on its network to share patient data, access medical records, use healthcare applications, and connect various departments efficiently.

The study highlights the main technologies and methods used in the hospital's network infrastructure. These include high-speed fiber optic cables for faster communication, VMware for server virtualization to reduce hardware dependency, and static IP addresses for better control and management of devices. It also explains how the hospital uses network segmentation to organize traffic, firewalls to protect against threats, and layered switching to improve performance and scalability.

In addition to connectivity and performance, the case study looks at how the hospital maintains network security, manages data backups, and ensures system reliability in case of failures. These strategies help avoid disruptions and ensure that critical services remain available at all times.

By identifying the strengths of the current setup and areas where improvements can be made, this report shows how a well-planned and managed network can improve hospital operations, enhance data protection, and prepare the system for future technology upgrades.

College of Engineering & Technology, Udyambag, Belagavi - 590 008, Karnataka, India
Ph.: 0831 - 2443881,82,83,0831-2440322 | Fax:0831-2441644| principal@klescet.ac.in | www.klescet.ac.in

2.Network and Server Infrastructure Overview

2.1 Network Components Overview

The network infrastructure at KLES Dr. Prabhakar Kore Hospital & Medical Research Centre, Belagavi, is designed to support seamless communication, reliable connectivity, and secure data exchange across various departments. This section outlines the key components of the hospital's IT system

2.1.1 Data Center

The data center serves as the central hub of the hospital's IT infrastructure. All core servers, networking equipment, and virtual environments are housed here, providing centralized control and management.

2.1.2 Connectivity

- Primary and Redundant Optical Fiber Cables (OFC) link the data center to different hospital blocks, ensuring high-speed and stable connectivity.
- Redundant Links automatically take over during failures, maintaining uninterrupted network operations.

2.1.3 Switching Infrastructure

- Layer 3 Core Switches are installed in the data center to manage routing and advanced traffic control.
- Layer 2 Distribution Switches are deployed in individual blocks to extend connectivity to departments.
- Structured Cabling using CAT5e, CAT6, and CAT6A cables connects endpoint devices (e.g., computers, printers) to the network efficiently.

College of Engineering & Technology, Udyambag, Belagavi - 590 008, Karnataka, India
Ph.: 0831 - 2443881,82,83,0831-2440322 | Fax:0831-2441644| principal@klescet.ac.in | www.klescet.ac.in

2.1.4 Virtualization

- The hospital uses VMware-based virtualization with two physical hosts connected to a Storage Area Network (SAN).
- Auto-migration of virtual machines between hosts minimizes downtime, reducing potential disruption from hours to just 3–4 minutes.

2.1.5 Network Topology & IP Addressing

- A Class B IP addressing scheme is used, with static IP assignments based on floor-wise distribution to simplify management and troubleshooting.
- DHCP is not used, reducing the risk of unauthorized access.
- The network currently supports around 600 connected devices.

2.2 Security Measures

2.2.1 Firewalls

- Two dedicated firewalls secure the network:
  - One for LAN users
  - One for Wi-Fi users, with user authentication and a captive portal
- Firewall functionalities include:
  - Bandwidth monitoring
  - Access control policies
  - Gateway-level filtering
  - Zero-day threat protection

2.2.2 Network Segmentation

- The hospital network is segmented into different zones:
  - LAN
  - Wi-Fi
  - CCTV network (isolated to prevent video traffic from affecting other services)

2.2.3 Domain Controller and DNS

- A centralized domain controller manages user authentication and access.
- DNS services support both forward and reverse lookups.
- Role-based access controls restrict actions like USB usage to enhance endpoint security.

2.2.4 Backup and Disaster Recovery

- Incremental backups are taken hourly, with a full backup scheduled daily at 1:15 AM.
- A three-tier backup strategy is implemented: hourly, daily, and weekly.
- Data is stored on 30 TB tapes, which are regularly rotated and also kept at an off-site location for disaster recovery.
- In case of host failure, virtual server failover occurs within minutes. If both hosts fail, manual migration is initiated.

3.Problems and Solutions

3.1 Problem

Lack of Firewall Redundancy and Manual Failover

In the current network setup at KLE Hospital, the firewall infrastructure comprises two Sophos firewall devices—one managing the LAN segment and the other handling Wi-Fi traffic. However, based on the topology blueprint and interviews with IT staff, it was identified that these firewalls operate independently without any configured High Availability (HA) mechanism. In the event of a firewall or routing failure, the failover process is manual and requires intervention from the Network Operations Center (NOC). This lack of automation can lead to prolonged service disruption, especially during emergencies or critical hours in medical care.

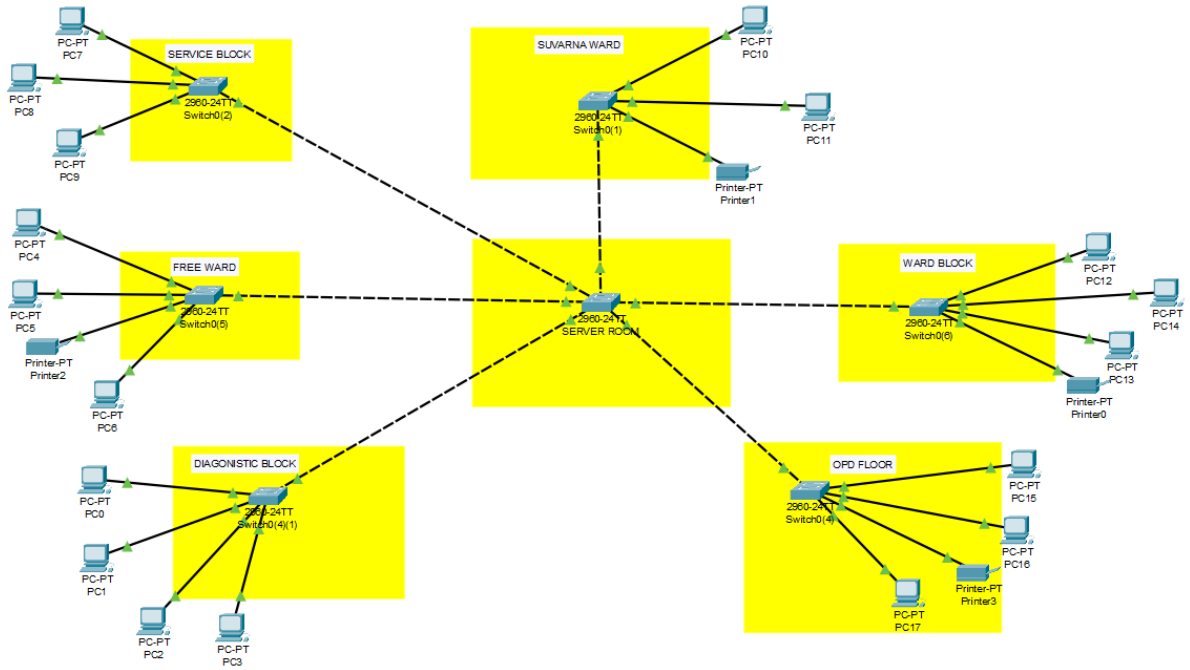

Fig 1. Current Hospital-Architecture

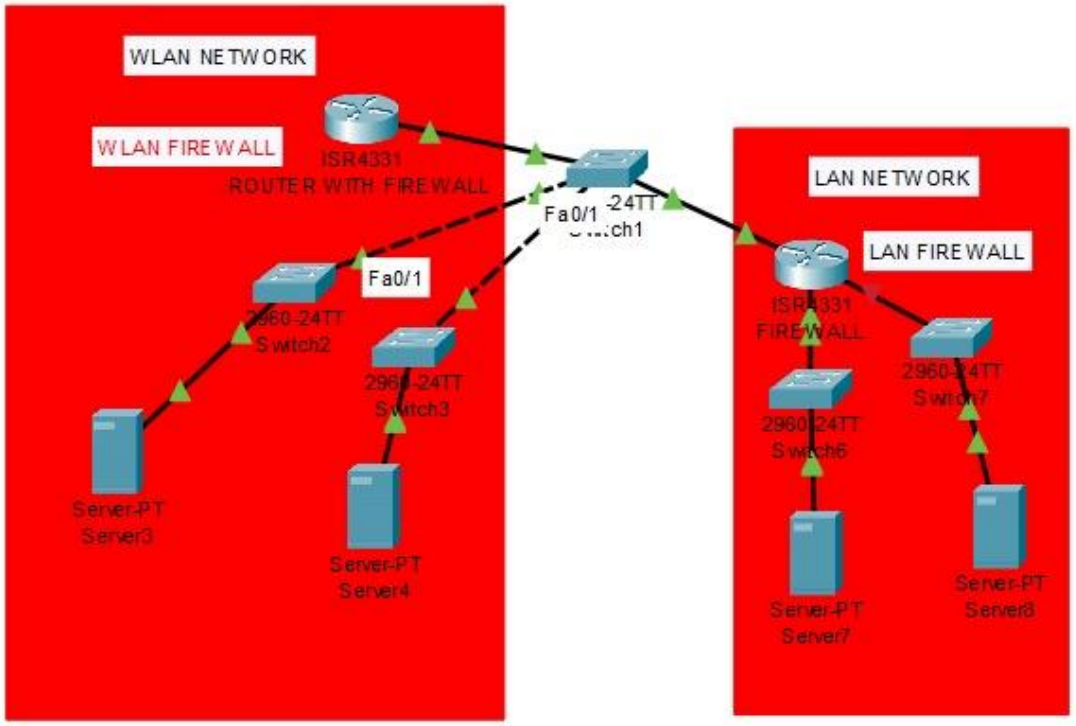

Fig 2. Current Hospital-Architecture of Server Room

A review of the network schematic reveals that while both main and redundant Optical Fiber Cable (OFC) paths are present across the hospital blocks, the firewalls are not clustered or synchronized. There is no physical or logical redundancy between the two firewall systems. The distribution network uses Cisco 9200 series switches with localized racks (6U to 15U), but no load balancer, virtual IP, or heartbeat communication is deployed between firewall units. Consequently, the hospital's current topology lacks resilience against device-level failure or misconfiguration, posing a significant risk to network continuity and patient service delivery.

College of Engineering & Technology, Udyambag, Belagavi - 590 008, Karnataka, India
Ph.: 0831 - 2443881,82,83,0831-2440322 | Fax:0831-2441644| principal@klescet.ac.in | www.klescet.ac.in

3.2 Solution

To address this issue, it is recommended to enable Active-Passive High Availability on the Sophos firewalls. In this setup, one firewall would act as the primary device while the secondary remains in standby mode. Heartbeat links should be configured over dedicated physical interfaces to ensure real-time synchronization and automatic failover. Sophos' native HA feature supports configuration mirroring and firmware synchronization, minimizing administrative overhead.

Additionally, implementing Sophos WAN Link Manager and SD-WAN profiles will allow intelligent traffic rerouting in case of uplink or device degradation. Gateway health monitoring using ICMP or HTTP probes can further automate switchover decisions. In the revised topology, both firewalls should be interconnected, and dual uplinks from the core switches should be routed through the HA pair. This will eliminate the current single points of failure while maintaining session continuity during firewall failover.

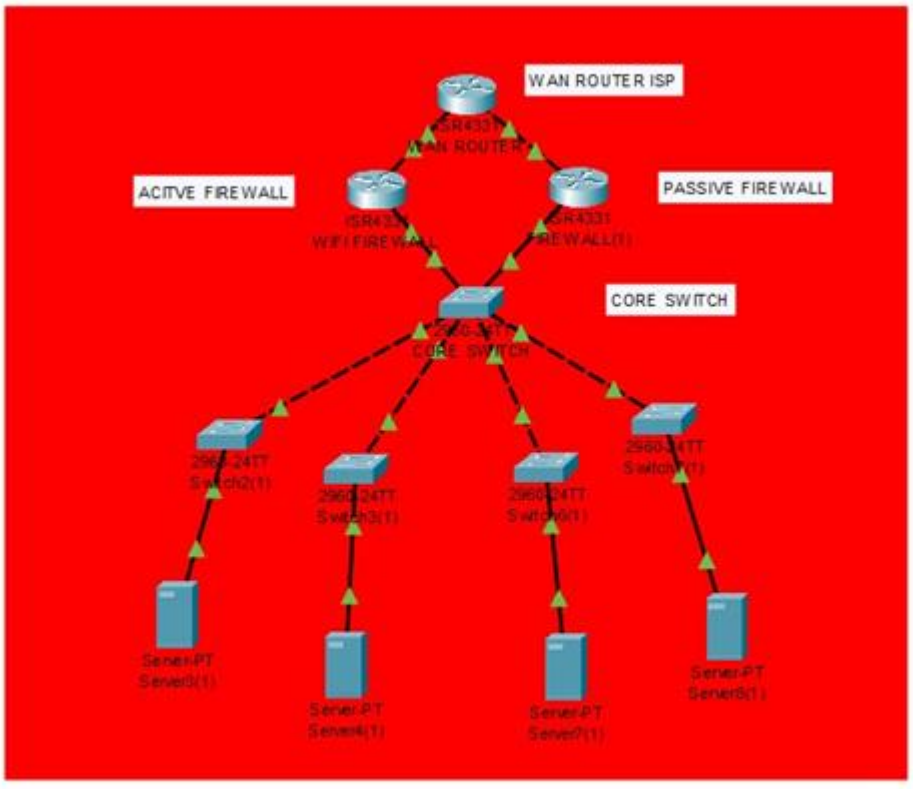

Fig 3. Suggested Hospital Architecture

In the medium term, deploying Sophos Central Firewall Manager (CFM) is advisable to streamline centralized policy management across network zones. The adoption of Zero Trust Network Access (ZTNA) and Sophos XDR will further enhance threat visibility and reduce lateral movement risks within the hospital's internal network.

By redesigning the network to incorporate HA-enabled Sophos firewalls and leveraging the existing OFC infrastructure effectively, KLE Hospital can significantly improve its network resilience, reduce NOC workload during failures, and ensure uninterrupted access to critical healthcare services.

College of Engineering & Technology, Udyambag, Belagavi - 590 008, Karnataka, India
Ph.: 0831 - 2443881,82,83,0831-2440322 | Fax:0831-2441644| principal@klescet.ac.in | www.klescet.ac.in

4.Photos

College of Engineering & Technology, Udyambag, Belagavi - 590 008, Karnataka, India
Ph.: 0831 - 2443881,82,83,0831-2440322 | Fax:0831-2441644| principal@klescet.ac.in | www.klescet.ac.in

5.Conclusion

The current firewall setup at KLES Dr. Prabhakar Kore Hospital lacks automatic redundancy, requiring manual intervention during failures, which poses risks to continuous network availability critical for healthcare services. Implementing Active-Passive High Availability with synchronized firewalls, redundant heartbeat links, and automated failover would greatly enhance network resilience, minimize downtime, and reduce the IT team's workload. Additionally, adopting advanced management tools and security policies will further strengthen the hospital's infrastructure, ensuring reliable and secure operations to support uninterrupted patient care.

College of Engineering & Technology, Udyambag, Belagavi - 590 008, Karnataka, India
Ph.: 0831 - 2443881,82,83,0831-2440322 | Fax:0831-2441644| principal@klescet.ac.in | www.klescet.ac.in